PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-059323
(43)Date of publication of application : 25.02.2000

(51)Int.Cl. H04H 1/00
H04L 9/08
H04L 9/10
H04L 29/08
H04N 7/167

(21)Application number : 10-224825
(22)Date of filing : 07.08.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : NISHIMURA TAKUYA
IIZUKA HIROYUKI
YAMADA MASAZUMI
GOTO SHOICHI
TAKECHI HIDEAKI
USUKI NAOJI

(30)Priority

Priority number	Priority date	Priority country
10031847	13.02.1998	JP
10151586	01.06.1998	JP

(54) DIGITAL AV DATA TRANSMISSION UNIT, DIGITAL AV DATA RECEPTION UNIT, DIGITAL AV DATA TRANSMISSION/RECEPTION SYSTEM AND MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To appropriately perform data communication while being immune to forgery or alteration and considering the importance of data or class of a recognition method by receiving an authentication request and performing authentication based on one kind of authentication rule selected out of a means

storing plural authentication rules on the side of transmission based on the discriminated result of a data importance discriminating means.
SOLUTION: When an authentication requesting means 12 receives the authentication request, a data importance discriminating means 3 discriminates the importance of AV data 2 to be transmitted and classifies them according to CGMS values. A transmission side authentication selecting means 6 sends the optimum authentication rule, which is selected out of a means 5 storing plural authentication rules on the side of transmission, to a digital AV reception unit TV9. At a digital AV transmission unit STB1, the same authentication rule as the selected certification rule is selected and a reception side authentication means 13 and a transmission side authentication means 7 mutually perform the authentication. When the authentication is made successful, the AV data 2 to be transmitted are enciphered and transmitted while using a work key Kco16 and the received enciphered data are deciphered by a work key Kco17.

LEGAL STATUS

[Date of request for examination]	16.08.2001
[Date of sending the examiner's decision of rejection]	17.12.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	2003-000846
[Date of requesting appeal against examiner's decision of rejection]	14.01.2003
[Date of extinction of right]	

CLAIMS

[Claim(s)]
[Claim 1] A data importance judging means to judge the significance of digital AV data, and a transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, A transmitting-side authentication selection means to receive an authentication demand and to choose one kind of rule

from said transmitting-side two or more authentication rule storing means based on the judgment result of said data importance judging means, The digital AV data transmitting unit characterized by having at least the transmitting-side authentication means which attests based on the selected authentication rule.
[Claim 2] A data importance judging means to judge the significance of digital AV data, and a transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, A transmitting-side authentication selection means to receive an authentication demand and to choose one kind of rule from said transmitting-side two or more authentication rule storing means based on the judgment result of said data importance judging means, An authentication demand means to set the digital AV data transmitting unit which has at least the transmitting-side authentication means which attests based on the selected authentication rule as the communicative object, and to require said authentication, Said transmitting-side two or more authentication rule storing means and said same receiving-side two or more authentication rule storing means by which two or more authentication rules of a class were stored, A receiving-side authentication selection means to choose from said receiving-side two or more authentication rule storing means the same authentication rule as the predetermined authentication rule chosen with said transmitting-side authentication selection means, The digital AV data receiving unit characterized by having at least the receiving-side authentication means which attests based on said selected authentication rule by the receiving side.
[Claim 3] A data importance judging means to judge the significance of digital AV data, and a transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, A transmitting-side authentication selection means to receive an authentication demand and to choose one kind of rule from said transmitting-side two or more authentication rule storing means based on the judgment result of said data importance judging means, The digital AV transmitting unit which has at least the transmitting-side authentication means which attests based on the selected authentication rule, An authentication demand means to require said authentication, and said transmitting-side two or more authentication rule storing means and said same receiving-side two or more authentication rule storing means by which two or more authentication rules of a class were stored, A receiving-side authentication selection means to choose from said receiving-side two or more authentication rule storing means the same authentication rule as the predetermined authentication rule chosen with said transmitting-side authentication selection means, The digital AV data transceiver system characterized by having the digital AV data receiving unit which has at least the receiving-side authentication means which attests based on said selected authentication rule by the receiving side.
[Claim 4] A data importance judging means to judge the significance of digital AV data, and a management-criteria storing means by which predetermined management criteria were stored, A management-criteria reference decision means to determine

whether an authentication demand should be received and said management criteria of said management-criteria storing means should be referred to based on the judgment result of said data importance judging means, An authentication decision means to determine whether it should attest according to it with reference to said management criteria according to the determined result, and the class of authentication, The digital AV data transmitting unit characterized by having at least the authentication means which attests based on a predetermined authentication rule according to the decision of the authentication decision means.
[Claim 5] It is the digital AV data transceiver system according to claim 3 which said transmitting unit has each function of said receiving unit, and is characterized by said receiving unit having each function of said transmitting unit.
[Claim 6] The digital AV data transceiver system according to claim 5 characterized by connecting the transmitting unit which has the function of said receiving unit, or three receiving units or more of each other which have the function of said transmitting unit, and being able to exchange digital AV data of each other.
[Claim 7] A transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, A unit authentication rule information receiving means to receive the information about one kind of authentication rule which a digital AV data receiving unit has, It is based on the information about said authentication rule received with said unit authentication rule information receiving means. The digital AV transmitting unit equipped with the transmitting-side authentication rule ejection means which takes out the authentication rule which said digital AV data receiving unit has from said transmitting-side two or more authentication rule storing means, and a transmitting-side authentication means to perform said authentication based on it, at least.
[Claim 8] A transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, A unit authentication rule information receiving means to receive the information about one kind of authentication rule which a digital AV data receiving unit has, It is based on the information about said authentication rule received with said unit authentication rule information receiving means. The transmitting-side authentication rule ejection means which takes out the authentication rule which said digital AV data receiving unit has from said transmitting-side two or more authentication rule storing means, An authentication demand means to set the digital AV transmitting unit which has at least a transmitting-side authentication means to perform said authentication based on it as the communicative object, and to require said authentication, A receiving-side authentication rule storing means to store said one kind of of one's authentication rule, The digital AV data receiving unit characterized by having at least an authentication rule information transmitting means to transmit the information about said authentication rule, and the receiving-side authentication means which attests with said authentication rule between said transmitting units.

[Claim 9] A transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, A unit authentication rule information receiving means to receive the information about one kind of authentication rule which a digital AV data receiving unit has, It is based on the information about said authentication rule received with said unit authentication rule information receiving means. The transmitting-side authentication rule ejection means which takes out the authentication rule which said digital AV data receiving unit has from said transmitting-side two or more authentication rule storing means, The digital AV transmitting unit which has at least a transmitting-side authentication means to perform said authentication based on it, An authentication demand means to require said authentication, and a receiving-side authentication rule storing means to store said one kind of of one's authentication rule, The digital AV data transceiver system characterized by having the digital AV data receiving unit which has at least an authentication rule information transmitting means to transmit the information about said authentication rule, and the receiving-side authentication means which attests with said authentication rule between said transmitting units.
[Claim 10] An authentication demand is received from a management-criteria storing means by which predetermined management criteria were stored, and a digital AV data receiving unit. A management-criteria reference decision means to determine whether said management criteria of said management-criteria storing means should be referred to according to the class or significance of the digital AV data receiving unit, An authentication decision means to determine whether it should attest according to it with reference to said management criteria according to the determined result, and the class of authentication, The digital AV transmitting unit characterized by having at least the authentication means which attests based on a predetermined authentication rule according to the decision of the authentication decision means.
[Claim 11] Said management criteria are a digital AV transmitting unit according to claim 4 or 10 characterized by being the criteria list (CRL) which can identify a just digital AV data receiving unit unjustly.
[Claim 12] The digital AV data transceiver system according to claim 9 characterized by connecting said two or more receiving units to said transmitting unit, and being able to exchange digital AV data between said transmitting units.
[Claim 13] A transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, A data importance judging means to judge the significance of digital AV data, and a transmitting-side authentication selection means to choose one kind of authentication rule from said transmitting-side two or more authentication rule storing means based on the judgment result of said data importance judging means, A unit authentication rule information receiving means to receive the information about one kind of authentication rule which a single authentication digital AV data receiving unit has, It

is based on the information about said authentication rule received with said unit authentication rule information receiving means. The transmitting-side authentication ejection means which takes out the authentication rule which said single authentication digital AV data receiving unit has from said transmitting-side two or more authentication rule storing means, The digital AV data transmitting unit characterized by having at least the transmitting-side authentication means which attests based on the authentication rule acquired from said transmitting-side authentication selection means or said transmitting-side authentication ejection means.

[Claim 14] A transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, A data importance judging means to judge the significance of digital AV data, and a transmitting-side authentication selection means to choose one kind of authentication rule from said transmitting-side two or more authentication rule storing means based on the judgment result of said data importance judging means, A unit authentication rule information receiving means to receive the information about one kind of authentication rule which a single authentication digital AV data receiving unit has, It is based on the information about said authentication rule received with said unit authentication rule information receiving means. The transmitting-side authentication ejection means which takes out the authentication rule which said single authentication digital AV data receiving unit has from said transmitting-side two or more authentication rule storing means, The digital AV data transmitting unit which has at least the transmitting-side authentication means which attests based on the authentication rule acquired from said transmitting-side authentication selection means or said transmitting-side authentication ejection means, An authentication demand means to require said authentication, and said transmitting-side authentication rule storing means and said same receiving-side two or more authentication rule storing means by which two or more authentication rules of a class were stored, A receiving-side authentication selection means to choose from said receiving-side two or more authentication rule storing means the same authentication rule as the predetermined authentication rule chosen with said transmitting-side authentication selection means, The two or more authentication digital AV data receiving unit which has at least the receiving-side authentication means which attests based on said selected authentication rule by the receiving side, An authentication demand means to require authentication, and a receiving-side single authentication rule storing means to store one kind of one's authentication rule, An authentication rule information transmitting means to transmit the information about said authentication rule, The digital AV data transceiver system characterized by having the single authentication digital AV data receiving unit which has at least the receiving-side authentication means which attests with said authentication rule between said digital AV data transmitting units.

[Claim 15] It is the digital AV data transceiver system according to claim 14 which said two or more authentication digital AV data receiving unit has each function of said digital AV data transmitting unit, and is characterized by said digital AV data transmitting unit having each function of said two or more authentication digital AV data receiving unit.
[Claim 16] The digital AV data transceiver system according to claim 15 characterized by connecting two or more two or more authentication digital AV data receiving units of each other which have the function of the digital AV data transmitting unit which has each function of said two or more authentication digital AV data receiving unit, or said digital AV data transmitting unit, and connecting said two or more single authentication digital AV data receiving units, and being able to exchange digital AV data of each other.
[Claim 17] An encryption means to encipher digital AV data on two or more level which accepted the significance of the data, An authentication means to perform authentication demanded from the receiving unit which receives said enciphered digital AV data, A level judging means to judge the authentication level attested by the authentication means, As opposed to a demand of the decode information for decoding said enciphered digital AV data from said receiving unit The transmitting unit characterized by having a decode information selection means to transmit authentication level [finishing / said judgment], an EQC, and said decode information on the level not more than it to said receiving unit.
[Claim 18] A level decision means to determine authentication level required in order to decode the enciphered data which are received from the transmitting unit which transmits the digital AV data enciphered on two or more level which accepted the significance of data, The receiving unit characterized by having a decode information-requirements means to require the decode information over said authentication level and EQC, and said encryption data of the level not more than it of said transmitting unit as an authentication means to require authentication of the determined authentication level of said transmitting unit.
[Claim 19] An encryption means to encipher digital AV data on two or more level which accepted the significance of the data, An authentication means to perform authentication demanded from the receiving unit which receives said enciphered digital AV data, A level judging means to judge the authentication level attested by the authentication means, As opposed to a demand of the decode information for decoding said enciphered digital AV data from said receiving unit The transmitting unit which has a decode information selection means to transmit authentication level [finishing / said judgment], an EQC, and said decode information on the level not more than it to said receiving unit, A level decision means to determine authentication level required in order to decode the enciphered data which are received from the transmitting unit, An authentication means to require authentication of the determined authentication level of said transmitting unit, The digital AV data

transceiver system characterized by having the receiving unit which has a decode information-requirements means to require said authentication level and EQC, and the decode information on the level not more than it of said transmitting unit.
[Claim 20] An encryption means to encipher digital AV data on two or more level which accepted the significance of the data, An authentication means to perform authentication demanded from the receiving unit which receives said enciphered digital AV data, A level judging means to judge the authentication level attested by the authentication means, As opposed to a demand of the decode information for decoding said enciphered digital AV data from said receiving unit It has a decode information selection means to transmit authentication level [finishing / said judgment], an EQC, or the decode information on the level not more than it to said receiving unit. Said decode information selection means Next, they are that the demand is equivalent to authentication level [finishing / said judgment] when there is a demand of decode information from said receiving unit, or the transmitting unit characterized by transmitting the decode information demanded without performing said authentication procedure to said receiving unit when it is said decode information on the level not more than it.
[Claim 21] A level decision means to determine authentication level required in order to decode the enciphered data which are received from the transmitting unit which transmits the digital AV data enciphered on two or more level which accepted the significance of data, An authentication means to require authentication of the determined authentication level of said transmitting unit, It has a decode information-requirements means to require the decode information over said authentication level and EQC, or said encryption data of the level not more than it of said transmitting unit. Said decode information-requirements means It is the receiving unit characterized by requiring said decode information, without performing said authentication demand when requiring the level of said authentication, an EQC, or the decode information on the level not more than it of said transmitting unit.
[Claim 22] An encryption means to encipher digital AV data on two or more level which accepted the significance of the data, An authentication means to perform authentication demanded from the receiving unit which receives said enciphered digital AV data, A level judging means to judge the authentication level attested by the authentication means, As opposed to a demand of the decode information for decoding said enciphered digital AV data from said receiving unit It has a decode information selection means to transmit authentication level [finishing / said judgment], an EQC, or the decode information on the level not more than it to said receiving unit. Said decode information selection means Next, that the demand is equivalent to authentication level [finishing / said judgment] when there is a demand of decode information from said receiving unit or when it is said decode information on the level not more than it, and when The transmitting unit which transmits the decode information demanded without performing said authentication procedure to

said receiving unit, A level decision means to determine authentication level required in order to decode the enciphered data which are received from the transmitting unit, An authentication means to require authentication of the determined authentication level of said transmitting unit, It has a decode information-requirements means to require said authentication level and EQC, or the decode information on the level not more than it of said transmitting unit. Said decode information-requirements means It is the digital AV data transceiver system characterized by having the receiving unit which requires said decode information, without performing said authentication demand when requiring the level of said authentication, an EQC, or the decode information on the level not more than it of said transmitting unit.

[Claim 23] The digital AV data transmitting approach characterized by attesting, and judging the level of the authentication and transmitting each decode information on the encryption approach corresponding to the authentication approach of level lower than the authentication approach and it equivalent to the level to said receiving-side unit about the authentication demand sent from the receiving-side unit according to a demand of the decode information from said receiving-side unit.

[Claim 24] About the decode information requirements sent from the receiving-side unit, the level of the authentication corresponding to the demanded decode information is judged. Compare the level of the authentication performed in the past between the level and said receiving-side unit, and when the level of said judged authentication is level equivalent to the level of the past authentication, or lower The digital AV data transmitting approach characterized by transmitting said demanded decode information from said receiving-side unit.

[Claim 25] A transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, A transmitting-side private seal <DP N=0005> certificate selection means to choose one kind of authentication rule from the transmitting-side two or more authentication rule storing means, It is the digital AV data transmitting unit equipped with the transmitting-side authentication means which attests based on the selected authentication rule at least. Require authentication and one kind of authentication rule is chosen from said same receiving-side two or more authentication rule storing means as said transmitting-side two or more authentication rule storing means by which two or more authentication rules of a class were stored. The digital AV data receiving unit which attests based on the selected authentication rule Or selection of the authentication rule in said transmitting unit The unit which was performed based on the judgment result of the significance of data, and judged said significance the information about said selected authentication rule to the unit which does not judge significance Delivery, The unit which does not judge said significance is a digital AV data transmitting unit characterized by choosing the same authentication rule based on the information.

[Claim 26] As opposed to the digital AV data transmitting unit which chooses one kind

of authentication rule from a transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, and attests based on the selected authentication rule An authentication demand means to require authentication, and said transmitting-side two or more authentication rule storing means and said same receiving-side two or more authentication rule storing means by which two or more authentication rules of a class were stored, A receiving-side authentication selection means to choose one kind of authentication rule from said receiving-side two or more authentication rule storing means, It is the digital AV data receiving unit equipped with the receiving-side authentication means which attests based on the selected authentication rule at least. Selection of the authentication rule in said transmitting unit or a receiving unit The unit which was performed based on the judgment result of the significance of data, and judged said significance the information about said selected authentication rule to the unit which does not judge significance Delivery, The unit which does not judge said significance is a digital AV data receiving unit characterized by choosing the same authentication rule based on the information.

[Claim 27] A transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, A transmitting-side authentication selection means to choose one kind of authentication rule from the transmitting-side two or more authentication rule storing means, The digital AV transmitting unit which has at least the transmitting-side authentication means which attests based on the selected authentication rule, An authentication demand means to require said authentication, and said transmitting-side two or more authentication rule storing means and said same receiving-side two or more authentication rule storing means by which two or more authentication rules of a class were stored, A receiving-side authentication selection means to choose one kind of authentication rule from said receiving-side two or more authentication rule storing means, It has the digital AV data receiving unit which has at least the receiving-side authentication means which attests based on the selected authentication rule. Selection of the authentication rule in said transmitting unit or a receiving unit The unit which was performed based on the judgment result of the significance of data, and judged said significance the information about said selected authentication rule to the unit which does not judge significance Delivery, The unit which does not judge said significance is a digital AV data transceiver system characterized by choosing the same authentication rule based on the information.

[Claim 28] A transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, Require authentication, judge the significance of digital AV data, and it is based on the judgment result. One kind of authentication rule is chosen from said same receiving-side two or more authentication rule storing means as said transmitting-side two or more authentication rule storing means by which two or more authentication rules of a

class were stored. A transmitting-side authentication selection means to choose from said transmitting-side two or more authentication rule storing means the same rule as said authentication rule chosen in the digital AV data receiving unit which attests based on the selected authentication rule, The digital AV data transmitting unit characterized by having at least the transmitting-side authentication means which attests based on the selected authentication rule.

[Claim 29] The same authentication rule as the predetermined authentication rule chosen by the receiving side is chosen from a transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored. As opposed to the digital AV data transmitting unit which attests based on the selected authentication rule An authentication demand means to require authentication, and said transmitting-side two or more authentication rule storing means and said same receiving-side two or more authentication rule storing means by which two or more authentication rules of a class were stored, A data importance judging means to judge the significance of digital AV data, and a receiving-side authentication selection means to choose one kind of authentication rule from said receiving-side two or more authentication rule storing means based on the judgment result of the data importance judging means, The digital AV data receiving unit characterized by having at least the receiving-side authentication means which attests based on the selected authentication rule.

[Claim 30] A transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, A transmitting-side authentication selection means to choose the same rule as the predetermined authentication rule chosen from the transmitting-side two or more authentication rule storing means by the receiving side, The digital AV transmitting unit which has at least the transmitting-side authentication means which attests based on the selected authentication rule, An authentication demand means to require said authentication, and said transmitting-side two or more authentication rule storing means and said same receiving-side two or more authentication rule storing means by which two or more authentication rules of a class were stored, A data importance judging means to judge the significance of digital AV data, and a receiving-side authentication selection means to choose one kind of rule from said receiving-side two or more authentication rule storing means based on the judgment result of the data importance judging means, The digital AV data transceiver system characterized by having the digital AV data receiving unit which has at least the receiving-side authentication means which attests based on the selected authentication rule.

[Claim 31] The authentication means which attests by choosing one kind of authentication rule from two or more kinds of authentication rules, A management-criteria storing means by which the predetermined management criteria over a receiving unit were stored, It is the digital AV data transmitting unit equipped with an authentication judging means to judge whether it attests by receiving the

authentication demand from said receiving unit, and referring to said management criteria stored. When it has only the function attested only with the low authentication rule of the significance in which the receiving unit which performs said authentication demand cannot have said management criteria, said receiving unit It is what the identification information for said management criteria corresponding to the receiving unit is given from an external management pin center,large. The authentication judging means of said transmitting unit The digital AV data transmitting unit characterized by canceling said authentication when reception and its identification information become improper about said identification information on the occasion of said authentication demand.

[Claim 32] As opposed to the digital AV data transmitting unit which has an authentication judging means to judge whether it attests by referring to the predetermined management criteria over the receiving unit which receives the authentication demand from a receiving unit and is stored in the management-criteria storing means It has an authentication demand means to perform said authentication demand, and an authentication means to attest only with the low authentication rule of the significance which cannot have said management criteria. It is the digital AV data receiving unit with which the identification information for said management criteria corresponding to the receiving unit itself is given from an external management pin center,large. The authentication judging means of said transmitting unit The digital AV data receiving unit characterized by canceling said authentication when reception and its identification information become improper about said identification information on the occasion of said authentication demand.

[Claim 33] The authentication means which attests by choosing one kind of authentication rule from two or more kinds of authentication rules, A management-criteria storing means by which the predetermined management criteria over a receiving unit were stored, The digital AV data transmitting unit which has an authentication judging means to judge whether it attests by receiving the authentication demand from said receiving unit, and referring to said management criteria stored, It has an authentication demand means to perform said authentication demand, and an authentication means to attest only with the low authentication rule of the significance which cannot have said management criteria, to the transmitting unit. It has the digital AV data receiving unit with which the identification information for said management criteria corresponding to the receiving unit itself is given from an external management pin center,large. The authentication judging means of said transmitting unit The digital AV data transceiver system characterized by canceling said authentication when reception and its identification information become improper about said identification information on the occasion of said authentication demand.

[Claim 34] Said predetermined management criteria are a digital AV data transmitting unit according to claim 31 characterized by being the criteria list which can identify a just digital AV data receiving unit unjustly, and said identification information being ID

for said management criteria corresponding to said receiving unit, and the signature to the ID.
[Claim 35] Said authentication judging means is a digital AV data transmitting unit according to claim 34 characterized by canceling said authentication when there were few said ID and signatures and one side becomes improper.
[Claim 36] Said signature is claim 34 characterized by being what created by each receiving unit using the discernment ID beforehand added to the proper, or a digital AV data transmitting unit given in 35.
[Claim 37] Said predetermined management criteria are a digital AV data receiving unit according to claim 32 characterized by being the criteria list which can identify a just digital AV data receiving unit unjustly, and said identification information being ID for said management criteria corresponding to said receiving unit, and the signature to the ID.
[Claim 38] Said authentication judging means is a digital AV data receiving unit according to claim 37 characterized by canceling said authentication when there were few said ID and signatures and one side becomes improper.
[Claim 39] Said signature is claim 37 characterized by being what created by each receiving unit using the discernment ID beforehand added to the proper, or a digital AV data receiving unit given in 38.
[Claim 40] Said predetermined management criteria are a digital AV data transceiver system according to claim 33 characterized by being the criteria list which can identify a just digital AV data receiving unit unjustly, and said identification information being ID for said management criteria corresponding to said receiving unit, and the signature to the ID.
[Claim 41] Said authentication judging means is a digital AV data transceiver system according to claim 40 characterized by canceling said authentication when there were few said ID and signatures and one side becomes improper.
[Claim 42] Said signature is claim 40 characterized by being what created by each receiving unit using the discernment ID beforehand added to the proper, or a digital AV data transceiver system given in 41.
[Claim 43] The medium characterized by storing the program for realizing all or a part of functions which each component or step which a unit according to claim 1 to 42, a system, or the transmitting approach has has.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]

[Field of the Invention] This invention relates to AV system with the function which attests between AV equipment.
[0002]
[Description of the Prior Art] The system which attests between conventional AV equipment is explained using drawing 2 and drawing 3 .
[0003] First, in drawing 2 , the digital AV data transmitting unit STB 18 is equipped with a public key, a private key 20, the authentication means 19, digital interface D-I/F22, and the encryption means 19. The public key and private key 20 are connected to digital interface D-I/F22 through the authentication means 19. Moreover, the encryption means 19 could refer to the public key and the private key 20, and has connected them to the digital interface 22. The digital AV data receiving unit TV 23 possesses a public key, a private key 26, the authentication means 25, digital interface D-I/F24, and the decryption means 27. The public key and private key 26 are connected to digital interface D-I/F24 through the authentication means 25. Moreover, the decryption means 27 could refer to the public key and the private key 26, and has connected them to digital interface D-I/F24. Furthermore, digital interface D-I/F22 and digital interface D-I/F24 have composition which can perform an exchange of data mutually.
[0004] Next, actuation between the digital AV data transmitting unit STB 18 and the digital AV data receiving unit TV 23 is explained. First, the digital AV data receiving unit TV 23 advances an authentication demand. Then, an authentication demand reaches digital interface D-I/F22 which constitutes the digital AV data transmitting unit STB 18 through digital interface D-I/F24. With the authentication means 19, digital interface D-I/F22 are attested with reference to a public key and a private key 20 in response to an authentication demand. If attested in the digital AV data transmitting unit STB 18, in the encryption means 21, data will be enciphered and the enciphered data will be transmitted through digital interface D-I/F22. This is decoded with the decryption means 27 with reference to a public key and a private key 26 through digital interface D-I/F24.
[0005] If it does in this way, a function strong against forgery or an alteration is realizable. However, the authentication using a public key and a private key requires much time amount. In the case of the data which are not not much important, like news, time amount may be superfluously taken by authentication. Moreover, if only the data which can be copied are received like VTR, since a device does not require authentication with a strict digital AV data receiving unit by the case, in such a case, the futility of time amount produces it.
[0006] Next, in drawing 3 , the digital AV transmitting unit STB 28 possesses the common key 30, the authentication means 29, digital interface D-I/F32, and the encryption means 31. The common key 30 is connected to digital interface D-I/F32 through the authentication means 29. Moreover, the encryption means 31 could refer to the common key 30, and has connected it to the digital interface 32. The digital AV

data receiving unit TV 33 possesses the common key 36, the authentication means 35, the digital interface 34, and the decryption means 37. The common key 36 is connected to the digital interface 34 through the authentication means 35. Moreover, the decryption means 37 could refer to the common key 36, and has connected it to the digital interface 34. Furthermore, the digital interface 32 and the digital interface 34 have composition which can perform an exchange of data mutually.

[0007] Next, actuation between the digital AV data transmitting unit STB 28 and the digital AV data receiving unit TV 33 is explained. First, the digital AV receiving unit TV 33 advances an authentication demand. Then, an authentication demand reaches digital interface D-I/F32 which constitutes the digital AV transmitting unit STB 28 through digital interface D-I/F34. With the authentication means 29, digital interface D-I/F32 are attested with reference to the common key 30 in response to an authentication demand. If attested in the digital AV transmitting unit STB 28, in the encryption means 31, data will be enciphered and the enciphered data will be transmitted through digital interface D-I/F32. This is decoded with the DEJITA decryption means 37 with reference to the common key 36 through digital interface D-I/F34.

[0008] If it does in this way, data can be attested by short time amount. In the case of important data, a third party may view [however, / since the authentication using a common key is weak to forgery or an alteration] and listen to data on [, such as a film of new work,] copyright for nothing. Moreover, in order to display all the data received like TV, when it connects with the device which performs strict authentication, it can be necessary to correspond, and authentication with a strict digital AV data receiving unit may be required, and it may happen that the copyright of important data is not protected in such a case.

[0009]

[Problem(s) to be Solved by the Invention] Thus, the technical problem that authentication of the data which are not not much important takes much time amount, and the technical problem that the authentication is weak to forgery or an alteration in spite of being important data exist. Moreover, the technical problem that the futility of time amount arises when what does not require strict authentication depending on a digital AV data receiving unit exists and strict authentication is performed to such a unit, and the technical problem that copyright is not kept when what reverse takes strict authentication depending on a digital AV data receiving unit exists and authentication which is not strict is performed to such a unit exist. Furthermore, even when you need the data which are not strict after performing strict authentication and acquiring a cryptographic key by strict authentication and the authentication which is not strict for prevention of an unauthorized use, when a cryptographic key is prepared corresponding to each, it is necessary to perform anew authentication which is not strict. Moreover, in the case of the device in which a receiving side does not have the abatement function of a device, a transmitting side has the technical

problem that it has composition which cannot eliminate an inaccurate device.
[0010] The technical problem that authentication of the data which are not [of such the former] important takes much time amount to this invention, The important technical problem that authentication of **** is weak to forgery or an alteration in spite of being data, It aims at offering the unit which can transmit and receive data by the suitable authentication approach, a system, etc. in consideration of the classification of the authentication approach which the importance of data and a partner's equipment have in consideration of the technical problem that strictness required for authentication differs, with a unit etc.
[0011]
[Means for Solving the Problem] In order to solve the technical problem mentioned above, this invention of claim 1 A data importance judging means to judge the significance of digital AV data, and a transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, A transmitting-side authentication selection means to receive an authentication demand and to choose one kind of rule from transmitting-side two or more authentication rule storing means based on the judgment result of a data importance judging means, It is the digital AV data transmitting unit equipped with the transmitting-side authentication means which attests based on the selected authentication rule at least.
[0012] Moreover, a data importance judging means by which this invention of claim 2 judges the significance of digital AV data, A transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, A transmitting-side authentication selection means to receive an authentication demand and to choose one kind of rule from transmitting-side two or more authentication rule storing means based on the judgment result of a data importance judging means, An authentication demand means to set the digital AV data transmitting unit which has at least the transmitting-side authentication means which attests based on the selected authentication rule as the communicative object, and to require authentication, Transmitting-side two or more authentication rule storing means and a receiving-side two or more authentication rule storing means by which two or more kinds of same authentication rules were stored, A receiving-side authentication selection means to choose from receiving-side two or more authentication rule storing means the same authentication rule as the predetermined authentication rule chosen with the transmitting-side authentication selection means, It is the digital AV data receiving unit equipped with the receiving-side authentication means which attests based on the authentication rule chosen by the receiving side at least.
[0013] Moreover, a data importance judging means by which this invention of claim 3 judges the significance of digital AV data, A transmitting-side two or more authentication rule storing means by which two or more kinds of authentication rules were stored, A transmitting-side authentication selection means to receive an

authentication demand and to choose one kind of rule from transmitting-side two or more authentication rule storing means based on the judgment result of a data importance judging means, The digital AV transmitting unit which has at least the transmitting-side authentication means which attests based on the selected authentication rule, An authentication demand means to require authentication, and transmitting-side two or more authentication rule storing means and a receiving-side two or more authentication rule storing means by which two or more kinds of same authentication rules were stored, A receiving-side authentication selection means to choose from receiving-side two or more authentication rule storing means the same authentication rule as the predetermined authentication rule chosen with the transmitting-side authentication selection means, It is the digital AV data transceiver system equipped with the digital AV data receiving unit which has at least the receiving-side authentication means which attests based on the authentication rule chosen by the receiving side.

[0014] Moreover, a data importance judging means by which this invention of claim 4 judges the significance of digital AV data, A management-criteria storing means by which predetermined management criteria were stored, and a management-criteria reference decision means to determine whether an authentication demand should be received and the management criteria of a management-criteria storing means should be referred to based on the judgment result of a data importance judging means, An authentication decision means to determine whether it should attest according to it with reference to management criteria according to the determined result, and the class of authentication, It is the digital AV data transmitting unit equipped with the authentication means which attests based on a predetermined authentication rule at least according to the decision of the authentication decision means.

[0015] Moreover, in this invention of claim 5, a transmitting unit has each function of a receiving unit, and a receiving unit is a digital AV data transceiver system according to claim 3 which has each function of a transmitting unit.

[0016] Moreover, this invention of claim 6 is the digital AV data transceiver system according to claim 5 which the transmitting unit which has the function of a receiving unit, or three receiving units or more of each other which have the function of a transmitting unit are connected, and can exchange digital AV data of each other.

[0017] Moreover, a transmitting-side two or more authentication rule storing means by which this invention of claim 7 stored two or more kinds of authentication rules, A unit authentication rule information receiving means to receive the information about one kind of authentication rule which a digital AV data receiving unit has, The transmitting-side authentication rule ejection means which takes out the authentication rule which a digital AV data receiving unit has from transmitting-side two or more authentication rule storing means based on the information about the authentication rule received with the unit authentication rule information receiving means, It is the digital AV transmitting unit equipped with the transmitting-side

authentication means which attests based on it at least. Moreover, a transmitting-side two or more authentication rule storing means by which this invention of claim 8 stored two or more kinds of authentication rules, A unit authentication rule information receiving means to receive the information about one kind of authentication rule which a digital AV data receiving unit has, The transmitting-side authentication rule ejection means which takes out the authentication rule which a digital AV data receiving unit has from transmitting-side two or more authentication rule storing means based on the information about the authentication rule received with the unit authentication rule information receiving means, An authentication demand means to set the digital AV transmitting unit which has at least the transmitting-side authentication means which attests based on it as the communicative object, and to require authentication, It is the digital AV data receiving unit equipped with a receiving-side authentication rule storing means to store one kind of one's authentication rule, an authentication rule information transmitting means to transmit the information about an authentication rule, and the receiving-side authentication means that attests with an authentication rule between transmitting units at least.

[0018] Moreover, a transmitting-side two or more authentication rule storing means by which this invention of claim 9 stored two or more kinds of authentication rules, A unit authentication rule information receiving means to receive the information about one kind of authentication rule which a digital AV data receiving unit has, The transmitting-side authentication rule ejection means which takes out the authentication rule which a digital AV data receiving unit has from transmitting-side two or more authentication rule storing means based on the information about the authentication rule received with the unit authentication rule information receiving means, The digital AV transmitting unit which has at least the transmitting-side authentication means which attests based on it, An authentication demand means to require authentication, and a receiving-side authentication rule storing means to store one kind of one's authentication rule, It is the digital AV data transceiver system equipped with the digital AV data receiving unit which has at least an authentication rule information transmitting means to transmit the information about an authentication rule, and the receiving-side authentication means which attests with an authentication rule between transmitting units.

[0019] Moreover, a management-criteria storing means by which this invention of claim 10 stored predetermined management criteria, A management-criteria reference decision means to determine whether the management criteria of a management-criteria storing means should be referred to in response to an authentication demand according to the class or significance of the digital AV data receiving unit from a digital AV data receiving unit, An authentication decision means to determine whether it should attest according to it with reference to management criteria according to the determined result, and the class of authentication, It is the digital AV transmitting

unit equipped with the authentication means which attests based on a predetermined authentication rule at least according to the decision of the authentication decision means.

[0020] Moreover, this invention of claim 11 is a digital AV transmitting unit according to claim 4 or 10 which is the criteria list (CRL) which can identify a just digital AV data receiving unit unjustly [management criteria].

[0021] Moreover, this invention of claim 12 is the digital AV data transceiver system according to claim 9 which two or more receiving units are connected to a transmitting unit, and can exchange digital AV data between transmitting units.

[0022] Moreover, a transmitting-side two or more authentication rule storing means by which this invention of claim 13 stored two or more kinds of authentication rules, A data importance judging means to judge the significance of digital AV data, and a transmitting-side authentication selection means to choose one kind of authentication rule from transmitting-side two or more authentication rule storing means based on the judgment result of a data importance judging means, A unit authentication rule information receiving means to receive the information about one kind of authentication rule which a single authentication digital AV data receiving unit has, The transmitting-side authentication ejection means which takes out the authentication rule which a single authentication digital AV data receiving unit has from transmitting-side two or more authentication rule storing means based on the information about the authentication rule received with the unit authentication rule information receiving means, It is the digital AV data transmitting unit equipped with the transmitting-side authentication means which attests based on the authentication rule acquired from the transmitting-side authentication selection means or the transmitting-side authentication ejection means at least.

[0023] Moreover, a transmitting-side two or more authentication rule storing means by which this invention of claim 14 stored two or more kinds of authentication rules, A data importance judging means to judge the significance of digital AV data, and a transmitting-side authentication selection means to choose one kind of authentication rule from transmitting-side two or more authentication rule storing means based on the judgment result of a data importance judging means, A unit authentication rule information receiving means to receive the information about one kind of authentication rule which a single authentication digital AV data receiving unit has, The transmitting-side authentication ejection means which takes out the authentication rule which a single authentication digital AV data receiving unit has from transmitting-side two or more authentication rule storing means based on the information about the authentication rule received with the unit authentication rule information receiving means, The digital AV data transmitting unit which has at least the transmitting-side authentication means which attests based on the authentication rule acquired from the transmitting-side authentication selection means or the transmitting-side authentication ejection means, An authentication demand means to

require authentication, and a transmitting-side authentication rule storing means and a receiving-side two or more authentication rule storing means by which two or more kinds of same authentication rules were stored, A receiving-side authentication selection means to choose from receiving-side two or more authentication rule storing means the same authentication rule as the predetermined authentication rule chosen with the transmitting-side authentication selection means, The two or more authentication digital AV data receiving unit which has at least the receiving-side authentication means which attests based on the authentication rule chosen by the receiving side, An authentication demand means to require authentication, and a receiving-side single authentication rule storing means to store one kind of one's authentication rule, An authentication rule information transmitting means to transmit the information about an authentication rule, It is the digital AV data transceiver system equipped with the single authentication digital AV data receiving unit which has at least the receiving-side authentication means which attests with an authentication rule between digital AV data transmitting units.

[0024] Moreover, in this invention of claim 15, a two or more authentication digital AV data receiving unit has each function of a digital AV data transmitting unit, and a digital AV data transmitting unit is a digital AV data transceiver system according to claim 14 which has each function of a two or more authentication digital AV data receiving unit.

[0025] Moreover, this invention of claim 16 is the digital AV data transceiver system according to claim 15 which two or more two or more authentication digital AV data receiving units of each other which have the function of the digital AV data transmitting unit which has each function of a two or more authentication digital AV data receiving unit, or a digital AV data transmitting unit are connected, and two or more single authentication digital AV data receiving units are connected, and can exchange digital AV data of each other.

[0026] An encryption means by which this invention of claim 17 enciphers digital AV data on two or more level which accepted the significance of the data, The authentication means which attests authentication level demanded from the receiving unit which receives the enciphered digital AV data, A level judging means to judge the authentication level attested by the authentication means, As opposed to a demand of the decode information for decoding the digital AV data enciphered from the receiving unit after authentication It is the transmitting unit equipped with a decode information selection means to transmit all or a part of authentication level [finishing / a judgment], EQC, and decode information on the level not more than it to a receiving unit.

[0027] A level decision means to determine authentication level required in order that this invention of claim 18 may decode the enciphered data which were received from the transmitting unit which transmits the digital AV data enciphered on two or more level which accepted the significance of data, An authentication means to require

authentication of the determined authentication level of a transmitting unit, It is the receiving unit equipped with a decode information-requirements means to require all or a part of decode information over authentication level, an EQC, and the encryption data of the level not more than it of a transmitting unit, after authentication by the transmitting unit.

[0028] An encryption means by which this invention of claim 19 enciphers digital AV data on two or more level which accepted the significance of the data, The authentication means which attests authentication level demanded from the receiving unit which receives the enciphered digital AV data, A level judging means to judge the authentication level attested by the authentication means, As opposed to a demand of the decode information for decoding the digital AV data enciphered from the receiving unit after authentication The transmitting unit which has a decode information selection means to transmit all or a part of authentication level [finishing / a judgment], EQC, and decode information on the level not more than it to a receiving unit, A level decision means to determine authentication level required in order to decode the enciphered data which were received from the transmitting unit, An authentication means to require authentication of the determined authentication level of a transmitting unit, It is the digital AV data transceiver system equipped with the receiving unit which has a decode information-requirements means to require all or a part of authentication level, EQC, and decode information on the level not more than it of a transmitting unit after authentication by the transmitting unit.

[0029] An encryption means by which this invention of claim 20 enciphers digital AV data on two or more level which accepted the significance of the data, The authentication means which attests authentication level demanded from the receiving unit which receives the enciphered digital AV data, A level judging means to judge the authentication level attested by the authentication means, As opposed to a demand of the decode information for decoding the digital AV data enciphered from the receiving unit after authentication It has a decode information selection means to transmit the decode information on level equivalent to authentication level [finishing / a judgment] to a receiving unit. A decode information selection means Next, when there is a demand of decode information from a receiving unit, the demand is equivalent to authentication level [finishing / a judgment], or the transmitting unit which transmits the decode information which omitted authentication procedure and was demanded when it was the decode information on the level not more than it to a receiving unit.

[0030] A level decision means to determine authentication level required in order that this invention of claim 21 may decode the enciphered data which were received from the transmitting unit which transmits the digital AV data enciphered on two or more level which accepted the significance of data, An authentication means to require authentication of the determined authentication level of a transmitting unit, It has a decode information-requirements means to require the decode information over the

encryption data of level equivalent to authentication level of a transmitting unit, after authentication by the transmitting unit. A decode information-requirements means When requiring the level of authentication, an EQC, or the decode information on the level not more than it of a transmitting unit, it is the receiving unit which requires decode information, without performing an authentication demand.
[0031] An encryption means by which this invention of claim 22 enciphers digital AV data on two or more level which accepted the significance of the data, The authentication means which attests authentication level demanded from the receiving unit which receives the enciphered digital AV data, A level judging means to judge the authentication level attested by the authentication means, As opposed to a demand of the decode information for decoding the digital AV data enciphered from the receiving unit after authentication It has a decode information selection means to transmit the decode information on level equivalent to authentication level [finishing / a judgment] to a receiving unit. A decode information selection means Next, that the demand is equivalent to authentication level [finishing / a judgment] when there is a demand of decode information from a receiving unit or when it is the decode information on the level not more than it, and when The transmitting unit which transmits the decode information which omitted authentication procedure and was demanded to a receiving unit, A level decision means to determine authentication level required in order to decode the enciphered data which were received from the transmitting unit, An authentication means to require authentication of the determined authentication level of a transmitting unit, It has a decode information-requirements means to require the decode information on level equivalent to authentication level of a transmitting unit, after authentication by the transmitting unit. A decode information-requirements means When requiring the level of authentication, an EQC, or the decode information on the level not more than it of a transmitting unit, it is the digital AV data transceiver system equipped with the receiving unit which has ** which requires decode information, without performing an authentication demand.
[0032] A transmitting-side two or more authentication rule storing means by which this invention of claim 25 stored two or more kinds of authentication rules, A transmitting-side authentication selection means to choose one kind of authentication rule from the transmitting-side two or more authentication rule storing means, It is the digital AV data transmitting unit equipped with the transmitting-side authentication means which attests based on the selected authentication rule at least. Require authentication and one kind of authentication rule is chosen from a receiving-side two or more authentication rule storing means by which two or more kinds of same authentication rules as transmitting-side two or more authentication rule storing means were stored. The digital AV data receiving unit which attests based on the selected authentication rule Or selection of the authentication rule in a transmitting unit The information about the authentication rule which the unit which was performed based on the judgment result of the significance of data, and judged

significance chose as the unit which does not judge significance Delivery, The unit which does not judge significance is a digital AV data transmitting unit which chooses the same authentication rule based on the information.
[0033] A transmitting-side two or more authentication rule storing means by which this invention of claim 28 stored two or more kinds of authentication rules, Require authentication, judge the significance of digital AV data, and it is based on the judgment result. One kind of authentication rule is chosen from a receiving-side two or more authentication rule storing means by which two or more kinds of same authentication rules as transmitting-side two or more authentication rule storing means were stored. A transmitting-side authentication selection means to choose from transmitting-side two or more authentication rule storing means the same rule as the authentication rule chosen in the digital AV data receiving unit which attests based on the selected authentication rule, It is the digital AV data transmitting unit equipped with the transmitting-side authentication means which attests based on the selected authentication rule at least.
[0034] The authentication means which attests by this invention of claim 31 choosing one kind of authentication rule from two or more kinds of authentication rules, A management-criteria storing means by which the predetermined management criteria over a receiving unit were stored, It is the digital AV data transmitting unit equipped with an authentication judging means to judge whether it attests by receiving the authentication demand from a receiving unit and referring to the management criteria stored. When it has only the function attested only with the low authentication rule of the significance in which the receiving unit which performs an authentication demand cannot have management criteria, a receiving unit It is what the identification information for management criteria corresponding to the receiving unit is given from an external management pin center,large. The authentication judging means of a transmitting unit When reception and its identification information become improper about identification information on the occasion of an authentication demand, it is the digital AV data transmitting unit which cancels authentication.
[0035] This invention of claim 43 is the medium which stored the program for realizing all or a part of functions which each component or step which a unit according to claim 1 to 42, a system, or the transmitting approach has has.
[0036]
[Embodiment of the Invention] The gestalt of operation of this invention is explained with reference to a drawing below.
[0037] First, the gestalt of the first operation is explained with reference to drawing 1 .
[0038] The digital AV data transmitting unit STB 1 has the data importance judging means 3, the encryption means 4, transmitting-side two or more authentication rule storing means 5, the transmitting-side authentication selection means 6, the transmitting-side authentication means 7, and digital interface D-I/F8. this data

importance judging means 3 -- the importance of data 2 -- significance -- responding -- two or more kinds -- a case -- a division -- carrying out -- a means -- it is . The significance of this data is expressed by CGMS. This CGMS exists in the interior or the header of the data sent from a broadcasting station. The encryption means 4 is a means to encipher data 2 with the work-piece key Kco16 created in process of authentication. The authentication approach which generates the work-piece key Kco16 is mentioned later. Transmitting-side two or more authentication rule storing means 5 is a means with two or more kinds of authentication rules. For example, they are two kinds of authentication rules, the authentication rule using a public key and a private key, and the authentication rule using a common key. Here, explanation is advanced noting that the authentication rule which used the public key and the private key, and the authentication rule using a common key are stored. The transmitting-side authentication selection means 6 is a means to choose one kind of authentication rule from two or more kinds of authentication rules which transmitting-side two or more authentication rule storing means 5 has. Under the present circumstances, it refers to the result of a judgment of the data importance judging means 3. Although the authentication rule using the public key and the private key as an authentication rule strong against forgery or an alteration is chosen although time amount is taken, and time amount is not taken by whether the aforementioned significance is high or low with the gestalt of this operation, the authentication rule using the common key as a weak rule is chosen as forgery or an alteration. The transmitting-side authentication means 7 is a means which exchanges the digital AV data receiving unit TV 9 and authentications actually with the selected authentication rule. Digital interface D-I/F8 is a means to perform an exchange of the digital AV data receiving unit TV 9, AV data, and a signal.

[0039] The digital AV data receiving unit TV 9 has digital interface D-I/F10, the decryption means 11, the authentication demand means 12, the receiving-side authentication means 13, receiving-side two or more authentication rule storing means 14, and the receiving-side authentication selection means 15. This authentication demand means 12 is a means which gives an authentication demand to the digital AV data transmitting unit STB 1. Moreover, receiving-side two or more authentication rule storing means 14 is a means with the authentication rule of two or more same classes as two or more authentication rules stored in transmitting-side two or more authentication rule storing means 5. Therefore, in the case of the gestalt of this operation, it has an authentication rule using the authentication rule and common key using a public key and a private key. The receiving-side authentication selection means 15 is a means to choose the same authentication rule as the authentication rule chosen with the transmitting-side authentication selection means 6 from receiving-side two or more authentication rule storing means 14 mentioned above. The receiving-side authentication means 13 is the selected authentication rule, that is, is a means which exchanges mutually the digital AV data transmitting unit

STB 1 and authentications actually using the authentication rule chosen in the digital AV data transmitting unit STB 1. The decryption means 11 is a means to decrypt the digital AV data enciphered and transmitted in the digital AV data transmitting unit STB 1 using the work-piece key Kco17. The work-piece key Kco17 is generated in said receiving-side authentication process, and mentions the approach of generating later with the approach of generating said work-piece key Kco16. Digital interface D-I/F10 is a means to perform an exchange of the transmitting unit STB 1, AV data, and a signal.

[0040] Next, actuation of the gestalt of such this operation is explained.

[0041] First, an authentication demand means 12 to constitute the digital AV data receiving unit TV 9 gives the authentication demands including its ID to the digital AV data transmitting unit STB 1 through digital interface D-I/F10. Of course, the Request to Send of AV data is also advanced. The digital AV data transmitting unit STB 1 receives said authentication demand through digital interface D-I/F8. the importance of that that is right, then the AV data 2 which the digital AV data transmitting unit STB 1 is the data importance judging means 3 first, and should be transmitted after this -- judging -- a case -- dividing -- carrying out . That is, if the value of CGMS is 11, significance is high, the data can only be displayed, and copying is forbidden. Moreover, when the value of CGMS is 10, it can copy once, and it is comparatively important data. Moreover, since you may view, listen, or copy and use it freely when CGMS is 00, it can be said to be unimportant data. Moreover, AV data with which CGMS is set to 01 do not exist. In the case of the significance of data, a division is made with the value of this CGMS. It is sent to the transmitting-side authentication selection means 6, and the optimal authentication rule is chosen from transmitting-side two or more authentication rule storing means 5 by this result. That is, in the case of important data, the newest film etc. requires time amount, but the authentication rule using a public key and a private key strong against forgery or an alteration is chosen. Moreover, in the case of unimportant data like news, although time amount is not taken, the weak authentication rule using a common key is chosen by forgery and alteration. Furthermore, the selection information is sent to the transmitting-side authentication means 7, and is sent to the digital AV receiving unit TV 9 through digital interface D-I/F8. In the digital AV receiving unit TV 9, the receiving-side authentication selection means 15 chooses from receiving-side two or more authentication rule storing means 14 the same authentication rule as the authentication rule chosen in the digital AV data transmitting unit STB 1 using the selection information. Therefore, the authentication rule chosen becomes the same by the transmitting side and the receiving side. Then, the receiving-side authentication means 13 and the transmitting-side authentication means 7 attest mutually through digital interface D-I/F10 and digital interface D-I/F8. If authentication is successful, as it mentions later, the work-piece key Kco16 will be generated by the transmitting side, and the work-piece key Kco17 will be generated by the receiving side. The data

2 which should be transmitted are enciphered with the encryption means 4 using the generated work-piece key Kco16. It is transmitted to the digital AV data receiving unit TV 9 as encryption data through digital interface D-I/F8 after it. Using the work-piece key Kco17, the data enciphered through digital interface D-I/F10 are decrypted with the decryption means 11, and turn into data 101. This is the same data as data 2, and it means that data were transmitted to the digital AV data receiving unit TV 9 from the digital AV data transmitting unit STB 1.

[0042] Finally, the digital AV data receiving unit TV 9 displays the data on the screen of a display unit. Thus, although time amount is taken when the importance of data is high, an authentication means strong against forgery or an alteration is used, and although time amount is not taken when the importance of data is low, a weak authentication rule is used for forgery or an alteration.

[0043] Next, as mentioned above, the exchange of authentication when an authentication demand appears from the digital AV data receiving unit TV 9 in the digital transmitting unit STB 1 is shown, and the gestalt of the operation which, as a result, generates the work-piece key Kco is explained with reference to drawing 4 and drawing 5 .

[0044] First, it is the case where come whenever it is shown in drawing 4 , and authentication by the public key and the private key is performed. In this case, a receiving side has a private key Sb and a public key Pb. Moreover, a transmitting side has a private key Sa and a public key Pa. A receiving side generates a random number B at step 1 first. A receiving side sends the cipher Sb (B) which enciphered IDb which is the recognition number of self, and a random number B with its private key Sb to a transmitting side. A transmitting side is searched from the recognition number IDb of a receiving side, and receives the public key Pb of a receiving side. Cipher Sb (B) is decrypted with the public key Pb which came to hand at step 8. As a result, a random number B is obtained like step 9. Furthermore, a transmitting side generates a random number A like step 10. Random numbers A and B are enciphered with the private key Sa of a transmitting side, and Cipher Sa (A, B) is created. A transmitting side transmits Cipher Sa (A, B) and the recognition number IDa of self to a receiving side. A receiving side receives the recognition number IDa of Cipher Sa (A, B) and a transmitting side. A receiving side is searched from the recognition number IDa of a transmitting side, receives the public key Pa of a transmitting side, and decrypts Cipher Sa (A, B) by Pa like step 2. Here, a receiving side understands that the random number B sent to the receiving side at step 1 and the completely same random number B are obtained from Cipher Sa (A, B), and neither forgery nor an alteration is performed. If said two random numbers differ, it turns out that it turns out that forgery and an alteration were performed and there is an inaccurate partner. However, public keys Pa and Pb shall come to hand no longer only to a just person in this case. Next, like step 3, a receiving side enciphers a random number A with the private key Sb of a receiving side, and creates Cipher Sb (A). Sb (A) is sent to a transmitting side

and decrypts Cipher Sb (A) like step 11 with the public key Pb of a receiving side which it already has by the transmitting side. If the random number B and the random number B decrypted at step 11 generated at step 10 are completely the same, a transmitting side understands that neither forgery nor an alteration is performed for it. If said two random numbers differ, it turns out that it turns out that forgery and an alteration were performed and there is an inaccurate partner.

[0045] Now, supposing, as for the random numbers A and B exchanged by the receiving side and the transmitting side, neither forgery nor an alteration is performed, random numbers A and B are random numbers of secrecy at the 3rd person other than a receiving side and a transmitting side. Then, by the transmitting side, Key Kab is created like step 12 using random numbers A and B. Similarly Key Kab is created using random numbers A and B by the receiving side like step 4. Said two Kab(s) are the same and completely serve as a common key. Next, Key Kex is created like step 13 by the transmitting side. This is enciphered with the common key Kab, Cipher Kab (Kex) is created, and it sends to a receiving side. The key Kex which the receiving side decrypted Cipher Kab (Kex) with the common key Kab like step 5, and obtained Kex, consequently the receiving side obtained, and the key Kex in a transmitting side are completely the same, and turn into a common key. Next, Key Kco is created like step 14 by the transmitting side. It is enciphered with the common key Kex and Key Kco is sent to a receiving side as a cipher Kex (Kco). In a receiving side, like step 6, Cipher Kex (Kco) is decrypted with the common key Kex, and Kco is obtained like step 7. The key Kco in a transmitting side and Kco in a receiving side are completely the same, and serve as a common key. The above is the work-piece key Kco obtained in process of authentication by the public key and the private key.

[0046] Next, it comes, whenever it is shown in drawing 5 , and the case where authentication with a common key is performed is explained. In this case, a transmitting side and a receiving side have the common key S. In addition, this common key is given only to the just person. First, two random numbers A1 and A2 are generated like step 15 in a receiving side, it enciphers with the common key S, Cipher S (A1A2) is created, and it sends to a transmitting side. In a transmitting side, Cipher S (A1A2) is decrypted with the common key S like step 20. If it does so, a random number A1 and a random number A2 will be obtained like step 21. A transmitting side sends a random number A2 to a receiving side. A receiving side will have two random numbers A1 and A2 like step 16. If the random number A2 received from the transmitting side at step 16 is completely the same as the random number A2 generated at step 15, it turns out that neither forgery nor an alteration is performed by the transmitting side. If the two above-mentioned random numbers differ, it will mean that forgery and an alteration were performed and authentication will go wrong. Next, like step 22, a transmitting side generates a random number B1 and B-2, enciphers and sends Cipher S (B1 B-2) to a receiving side. A receiving side decrypts Cipher S (B1 B-2) using the common key S like step 17. Then, a random

number B1 and B-2 are obtained like step 18. A receiving side sends random-number B-2 to a transmitting side. A transmitting side will have a random number B1 and B-2 like step 23. If random-number B-2 thought to be the random number generated at step 22 from the receiving side at step 23 is the same, it will turn out that neither forgery nor an alteration is performed to the receiving side, and authentication will be successful. If the two above-mentioned random numbers differ, it means that forgery and an alteration were performed and authentication is failure.

[0047] Here, supposing authentication was successful, a random number A1 and a random number B1 are random numbers of secrecy at the 3rd person other than a transmitting side and a receiving side. In a transmitting side, Key Kco is created from a random number A1 and a random number B1 like step 24. On the other hand by the receiving side, Key Kco is created from a random number A1 and a random number B1 like step 19. The key Kco in a transmitting side and the key Kco in a receiving side are completely the same, and are a common key. The above is the work-piece key Kco obtained in process of authentication with a common key.

[0048] In addition, in this invention, the class of not only two kinds of said public keys and private keys, and common keys but others is sufficient as the class of authentication rule to choose, and three more or more kinds of different authentication rules may be used for it.

[0049] Moreover, as a modification of the gestalt of this operation, the digital AV data transmitting unit 1 has the same function as the digital AV receiving unit 9, and the digital AV data receiving unit 9 has the same function as the digital AV transmitting unit 1. Those units are henceforth called a digital AV data transceiver unit. Moreover, you may connect mutually [those transceiver units] three or more sets.

[0050] Next, the gestalt of operation of the second of this invention is explained with reference to drawing 6 .

[0051] The place which chooses an authentication rule according to the class of authentication rule which the digital AV data receiving unit VTR 45 has with the gestalt of this operation to the gestalt of the first operation having changed the authentication rule according to the significance of data is a point of difference.

[0052] The digital AV data transmitting unit STB 38 has transmitting-side two or more authentication rule storing means 41 grade. Transmitting-side two or more authentication rule storing means 41 is a means with two or more kinds of authentication rules. This is an authentication rule using a public key and a private key, and an authentication rule using a common key, as the gestalt of the first operation explained. Here, explanation is advanced noting that the authentication rule which used the public key and the private key, and the authentication rule using a common key are stored. The unit authentication rule information receiving means 42 is a means to receive the information relevant to the authentication rule sent from the digital AV data receiving unit VTR 45. The transmitting-side authentication ejection means 53 is a means to pass a predetermined authentication rule to ejection

and the transmitting-side authentication means 43 based on the information relevant to the authentication rule from transmitting-side two or more authentication rule storing means 41. The transmitting-side authentication means 43 is a means which exchanges authentications with the digital AV receiving unit VTR 45 mutually. The encryption means 40 is a means to encipher data 39 with the work-piece key Kco53 generated as a result of exchanging authentications, as the gestalt of the first operation explained. Digital interface D-U/F44 are a means which carries out an exchange of the digital AV data receiving unit VTR 45, data, and a signal.

[0053] The digital AV data receiving unit VTR 45 has receiving-side authentication rule storing means 49 grade. This receiving-side authentication rule storing means 49 is a means to store only one kind of authentication rule unlike the case where the gestalt of the first operation explains. For example, there is an authentication rule like the authentication rule using a public key and a private key or the authentication rule using a common key. Here, the authentication rule stored in the receiving-side authentication rule storing means 49 is beforehand decided with the property or significance of equipment of the digital AV data receiving unit VTR 45. That is, although the authentication rule strong against forgery or an alteration is stored although units, such as TV which is not probably beforehand about reuse of data, take time amount, and time amount is not taken at a unit like VTR on condition of a copy of data, the authentication rule weak to forgery or an alteration is stored. The copyright of AV data can be kept by this. With the gestalt of this operation Since the digital AV data receiving unit VTR 45 is VTR, the receiving-side authentication rule storing means 49 explains as a thing with a common key. The authentication rule information transmitting means 50 is a means to transmit the information relevant to an authentication rule with the common key which the digital AV data receiving unit VTR 45 has for the receiving-side authentication rule storing means 49. The receiving-side authentication means 51 is a means which exchanges authentications with the digital AV transmitting unit STB 38 mutually. The decryption means 47 is a means to decrypt the enciphered data with the work-piece key Kco54 generated as a result of exchanging authentications, as the gestalt of the first operation explained.

[0054] Next, actuation of the gestalt of such this operation is explained.

[0055] First, an authentication demand means 48 to constitute the digital AV data receiving unit VTR 45 gives an authentication demand to the digital AV data transmitting unit STB 38 through digital interface D-I/F46. The digital AV data transmitting unit STB 38 receives said authentication demand through digital interface D-I/F44. Moreover, the authentication rule information transmitting means 50 takes out the information about the authentication rule stored, i.e., an authentication rule with a common key, with reference to the receiving-side authentication rule storing means 49 simultaneously. For example, the identifier which shows an authentication rule with the common key is sent to the digital AV data transmitting unit STB 38 through digital interface D-I/F46. The unit authentication rule information receiving

means 42 receives the identifier of the information about the authentication rule sent from the digital AV data receiving unit VTR 45, i.e., an authentication rule with a common key, through digital interface D-I/F44. Furthermore, the identifier of this authentication rule is passed to the transmitting-side authentication rule ejection means 55, and takes out the authentication rule according to the information about that authentication rule, i.e., an authentication rule with a common key, from transmitting-side two or more authentication rule storing means 41. Then, the authentication rule with the taken-out common key is passed to the transmitting-side authentication means 43. Then, the transmitting-side authentication means 43 and the receiving-side authentication means 51 exchange authentications through digital interface D-I/F44 and D-I/F46 mutually. If authentication is successful consequently, as the gestalt of the first operation explained, the work-piece key Kco53 will be generated by the transmitting side, and the work-piece key Kco54 will be generated by the receiving side. Data 39 are enciphered by the work-piece key Kco53 with the encryption means 40. The enciphered data are sent to the digital AV receiving unit VTR 45 through digital interface D-I/F44. The data enciphered through digital interface D-I/F46 are sent to the decryption means 47, it is decrypted using the work-piece key Kco54, and data 52 are obtained.

[0056] In addition, in this invention, the class of said not only common key but a public key, a private key, and others is sufficient as the class of authentication rule of a transmitting side, and three more or more kinds of different authentication rules may be used for it.

[0057] Moreover, it may have only an authentication rule [according / one of them / to a common key] according [a digital AV data receiving unit] to those with two set, and other one may have only a public key and a private key. You may be three more or more sets of digital AV data receiving units.

[0058] Next, the gestalt of operation of the third of this invention is explained with reference to drawing 7 .

[0059] The place which determines an authentication rule according to both the significance of data and the class of digital AV receiving unit with the gestalt of this operation to the gestalt of the second operation having changed the authentication rule according to the class of digital AV data receiving unit as opposed to the gestalt of the first operation having changed the authentication rule according to the significance of data is the description.

[0060] With the gestalt of this operation, three kinds of units, the digital AV data transmitting unit STB 56, the two or more authentication digital AV data receiving unit TV 65, and the single authentication digital AV data receiving unit VTR 72, are treated. The digital AV data transmitting unit STB 56 is a unit which transmits data to the two or more authentication digital AV data receiving unit TV 65 and the single authentication digital AV data receiving unit VTR 72. To the two or more authentication digital AV data receiving unit TV 65, in the digital AV data transmitting

unit STB 56, two or more kinds of authentication rules are chosen with the significance of data, and the data is transmitted. Moreover, the single authentication digital AV data receiving unit VTR 72 uses one authentication rule which oneself has, and is a digital AV data transmitting unit. It is the unit which attests by STB56.
[0061] The digital AV data transmitting unit STB 56 has the data importance judging means 57. This is a means which divides the importance of data 82 according to significance in the case of two or more kinds. This significance is expressed by CGMS, as the gestalt of the first operation explained. This CGMS exists in the interior or the header of the data sent from a broadcasting station. The encryption means 64 is a means to encipher data 82 with the work-piece key Kco79 created in process of authentication. The gestalt of the first operation explained the process which generates the work-piece key Kco79. Transmitting-side two or more authentication rule storing means 63 has two or more kinds of authentication rules. For example, they are an authentication rule using a public key and a private key, and an authentication rule using a common key. Here, explanation is advanced noting that the authentication rule which used the public key and the private key, and the authentication rule using a common key are stored. The transmitting-side authentication selection means 59 is a means to choose one kind of authentication rule from two or more kinds of authentication rules which transmitting-side two or more authentication rule storing means 63 has. In the case of the data importance judging means 57, it refers to the result of a division at this time. Although the authentication rule using the public key and the private key as an authentication rule strong against forgery or an alteration is chosen by whether the aforementioned significance is high or low with the gestalt of this operation although time amount is taken, and time amount is not taken like the gestalt of the first operation, the authentication rule using the common key as a weak authentication rule is chosen as forgery or an alteration. The unit authentication rule information receiving means 60 is a means to receive the information about the authentication rule sent from the single authentication digital AV data receiving unit VTR 72. The transmitting-side authentication rule ejection means 58 is a means to pass a predetermined authentication rule to ejection and the transmitting-side authentication means 61 based on the information relevant to an authentication rule from transmitting-side two or more authentication rule storing means 63. The transmitting-side authentication means 61 is a means which exchanges the two or more authentication digital AV data receiving unit TV 65 and the single authentication digital AV data receiving unit VTR 72, and authentications actually. Digital interface D-I/F62 is a means to exchange the two or more authentication digital AV data receiving unit TV 65, the single authentication digital AV data receiving unit VTR 72, AV data, and a signal.
[0062] The two or more authentication digital AV data receiving unit TV 65 has the authentication demand means 67. This is a means which gives an authentication

demand to the digital AV data transmitting unit STB 56. Moreover, receiving-side two or more authentication rule storing means 68 has two or more kinds of same authentication rules as transmitting-side two or more authentication rule storing means 63. Therefore, in the case of the gestalt of this operation, there is an authentication rule using the authentication rule and common key using a public key and a private key. The receiving-side authentication selection means 69 is a means to choose from receiving-side two or more authentication rule storing means 68 the same authentication rule as the authentication rule chosen with the transmitting-side authentication selection means 59. The receiving-side authentication means 70 is the selected authentication rule, that is, is a means which exchanges mutually the digital AV data transmitting unit STB 56 and authentications actually using the authentication rule chosen in the digital AV data transmitting unit STB 56. The decryption means 66 is a means to decrypt the digital AV data enciphered in the digital AV data transmitting unit STB 56 using the work-piece key Kco80. The work-piece key Kco80 is generated in said authentication process, and the approach of generating explained it with the gestalt of the first operation with said work-piece key Kco79. Digital interface D-I/F71 is a means to perform an exchange of the digital AV data transmitting unit STB 56, AV data, and a signal.

[0063] The single authentication digital AV data receiving unit VTR 72 has the receiving-side authentication rule storing means 75. This is a means to store only one kind of authentication rule as mentioned above. For example, there is an authentication rule like the authentication rule using a public key and a private key or the authentication rule using a common key. Here, the authentication rule stored in the receiving-side authentication rule storing means 75 is beforehand decided with the class of equipment of the single authentication digital AV data receiving unit VTR 72, and significance. Here, it explains as that in which the receiving-side authentication rule storing means 75 has a common key. The authentication rule information transmitting means 76 is a means to transmit the information relevant to an authentication rule with the common key which the single authentication digital AV data receiving unit VTR 72 has for the receiving-side authentication rule storing means 75. The receiving-side authentication means 77 is a means which exchanges authentications with the digital AV data transmitting unit STB 56 mutually. The decryption means 73 is a means to decrypt the enciphered data with the work-piece key Kco81 generated as a result of exchanging authentications, as the gestalt of the first operation explained.

[0064] Next, actuation of the gestalt of such this operation is explained. first, the start -- the two or more authentication digital AV data receiving unit TV 65 -- or the single authentication digital AV data receiving unit 72 advances an authentication demand. The digital AV data transmitting unit STB 56 judges from which unit the authentication demand has been sent.

[0065] The case where an authentication demand comes first from the two or more

authentication digital AV data receiving unit TV 65 is explained hereafter, and explanation when an authentication demand next comes from the single authentication digital AV data receiving unit VTR 72 is given.

[0066] In the first place, an authentication demand means 67 to constitute the two or more authentication digital AV data receiving unit TV 65 as mentioned above gives the authentication demands including its ID to the digital AV data transmitting unit STB 56 through digital interface D-I/F71. The digital AV data transmitting unit STB 56 receives said authentication demand through digital interface D-I/F62. that that is right, then the importance of data 82 which the digital AV data transmitting unit STB 56 is the data importance judging means 57 first, and should be transmitted after this -- judging -- a case -- dividing -- carrying out . It is sent to the transmitting-side authentication selection means 59, and the optimal authentication rule is chosen from transmitting-side two or more authentication rule storing means 63 by this result. That is, in the case of important data, the authentication rule which uses a public key and a private key is chosen. Moreover, in the case of unimportant data, the authentication rule which uses a common key is chosen. Furthermore, the selection information is sent to the transmitting-side authentication means 61, and is sent to the two or more authentication digital AV data receiving unit TV 65 through digital interface D-I/F62. In the two or more authentication digital AV data receiving unit TV 65, the receiving-side authentication selection means 69 chooses the same authentication rule as the authentication rule chosen from receiving-side two or more authentication rule storing means 68 in the digital AV data transmitting unit STB 56 using the selection information. Therefore, the authentication rule chosen becomes the same by the transmitting side and the receiving side. The receiving-side authentication means 70 and the transmitting-side authentication means 61 attest mutually through digital interface D-I/F71 and digital interface D-I/F62. If authentication is successful, as explained in full detail with the gestalt of the first operation, the work-piece key Kco79 will be generated by the transmitting side, and the work-piece key Kco80 will be generated by the receiving side. The data 82 which should be transmitted are enciphered with the encryption means 64 using the generated work-piece key Kco79. It is transmitted through digital interface D-I/F62 after it as data enciphered by the two or more authentication digital AV data receiving unit TV 65. Using the work-piece key Kco80, the data enciphered through digital interface D-I/F71 are decrypted with the decryption means 66, and turn into data 83. This is the same data as data 82, and it means that data were transmitted to the two or more authentication digital AV data receiving unit TV 65 from the digital AV data transmitting unit STB 56. Thus, although time amount is taken when the importance of data is high, an authentication rule strong against forgery or an alteration is used, and although time amount is not taken when the importance of data is low, a weak authentication rule is used for forgery or an alteration.

[0067] Next, actuation when an authentication demand comes from the single

authentication digital AV data receiving unit VTR 72 is explained. First, an authentication demand means 74 to constitute the single authentication digital AV data receiving unit VTR 72 gives an authentication demand to the digital AV data transmitting unit STB 56 through digital interface D-I/F78. The digital AV data transmitting unit STB 56 receives said authentication demand through digital interface D-I/F62. The authentication rule information transmitting means 76 takes out the information about the authentication rule stored, i.e., an authentication rule with a common key, with reference to the receiving-side authentication rule storing means 75 simultaneously. For example, the identifier which shows an authentication rule with the common key is sent to the digital AV data transmitting unit STB 56 through digital interface D-I/F78. The identifier of the information about the authentication rule to which the unit authentication rule information receiving means 60 has been sent from the single authentication digital AV data receiving unit VTR 72, i.e., an authentication rule with a common key, is passed to the identifier of this authentication rule by reception and the pan through digital interface D-I/F62 at the transmitting-side authentication rule ejection means 58. The transmitting-side authentication rule ejection means 58 passes the authentication rule according to the information about the authentication rule, i.e., an authentication rule with a common key, to ejection and the transmitting-side authentication means 61 from transmitting-side two or more authentication rule storing means 63. The transmitting-side authentication means 61 and the receiving-side authentication means 77 exchange authentications through digital interface D-I/F62 and D-I/F78 mutually. If authentication is successful consequently, as explained in full detail with the gestalt of the first operation, the work-piece key Kco79 will be generated by the transmitting side, and the work-piece key Kco81 will be generated by the receiving side. The process in which a work-piece key was generated as a result of authentication was explained in full detail with the gestalt of the first operation.

[0068] Data 82 are enciphered by the work-piece key Kco79 with the encryption means 64. The enciphered data are sent to the single authentication digital AV data receiving unit VTR 72 through digital interface D-I/F62. The enciphered data which were received through digital interface D-I/F78 are sent to the decryption means 73, it is decrypted using the work-piece key Kco81, and data 84 are obtained. This is the same data as data 82, and it means that data were transmitted to the single authentication digital AV data receiving unit VTR 72 from the digital AV data transmitting unit STB 56.

[0069] Next, the gestalt of operation of the fourth of this invention is explained.

[0070] With the gestalt of this operation, the management criteria (CRL) which investigated and created what has a just digital AV data receiving unit, or an inaccurate thing are used. The approach of creating based on the registration card which the dealer which the consumer purchased published etc. thinks, and the method of the creation of CRL is ******.

[0071] Drawing 8 determines whether refer to the management criteria according to the significance of the digital AV data with which the management criteria are sent from a broadcasting station.
[0072] The digital AV transmitting unit STB 93 has a data importance judging means 86 to judge the importance of data, according to the significance of the digital AV data sent from a broadcasting station. Moreover, it has a management-criteria reference decision means 87 to judge whether the management-criteria information (CRL) stored in the management-criteria storing means 88 according to the significance of data is referred to. Moreover, according to said decision result, it has an authentication decision means 89 to determine whether attest or not. Moreover, it has the authentication means 90 which exchanges the digital AV data receiving unit TV 92 and authentications actually. Said authentication means 90 is connected to the digital AV data receiving unit TV 92 through digital interface D-I/F91.
[0073] Next, actuation of the gestalt of this operation is explained. First, the digital AV data 85 sent from a broadcasting station are the data importance judging means 86, and have importance judged. The result is passed to the management-criteria reference decision means 87, and it is determined whether the information stored in the management-criteria storing means 88 should be referred to. For example, since it is important in the case of the film of new work etc., it determines to refer to management-criteria information. Moreover, since it is not important in the case of news etc., it determines not to refer to management-criteria information. Furthermore, it is determined whether, with the authentication decision means 89, it should attest according to the judgment decision of said management-criteria reference decision means 87. That is, the digital AV data receiving unit TV 92 is judged for the management-criteria information in which the device just although the digital AV data 85 are received, or the unjust device is stored by the management-criteria storing means 88. If it is judged that it is just, the digital AV receiving unit TV 92 and authentications will be exchanged through digital interface D-I/F91 with the following authentication means 90. If it is judged that it is unjust, at the event, authentications with the digital AV data receiving unit TV 92 will not be exchanged, and transmission of data 85 will not be carried out.
[0074] On the other hand, it is determined whether drawing 9 refers to the management criteria for the management criteria mentioned above according to the class of equipment of a digital AV data receiving unit, or significance.
[0075] The digital AV data transmitting unit STB 94 has a management-criteria reference decision means 95 to determine whether the management-criteria storing means 96 should be referred to, according to the class or significance of equipment of the digital AV data receiving unit VTR 100. Moreover, it determines whether attest the authentication decision means 97. The information on a just device or the device which is not just is stored in the digital AV data receiving unit VTR 100 receiving digital AV data, as for the management-criteria storing means 96. The authentication

means 98 is attested with the digital AV data receiving unit VTR 100 through digital interface D-I/F99.
[0076] Next, actuation of the gestalt of this operation is explained. First, the digital AV data receiving unit VTR 100 sends device information to the management-criteria reference decision means 95 through digital interface D-I/F99. In response, the management-criteria reference decision means 95 determines whether the information stored in the management-criteria storing means 96 should be referred to. When referring to the management-criteria storing means 96 is determined, the authentication decision means 97 judges a just device and an inaccurate device with reference to the management-criteria storing means 96 first, although a digital AV data receiving unit receives data. Here, if judged with a just device, a digital AV data receiving unit and authentication will be started through digital interface D-I/F99 with the following authentication means 98. Although data are received, when a digital AV data receiving unit is judged to be an inaccurate device, authentication is not performed and transmission of data is not performed, either.
[0077] In addition, with the gestalt of the above-mentioned implementation, although STB has been explained as a transmitting unit, in case the data recorded on videotape with VTR are reproduced, VTR serves as a transmitting unit. Under the present circumstances, if CGMS is "possible [a 1 time copy]" at the time of an input, it will be rewritten by "a copy is improper" and will be outputted. As a significance of data, the significance at the time of the original input should be considered here, and the same authentication rule as "a 1-time copy is good" can also be used. Thus, when it is necessary to recognize "the data it became impossible to copy as a result of the 1-time copy", and "data [that it cannot copy from a dimension]", the CGMS value 01 which was mentioned above and not existing can also be assigned to the former distinction.
[0078] Next, the gestalt of operation of the fifth of this invention is explained.
[0079] Drawing 10 is a schematic diagram about the gestalt of operation of the fifth of this invention. With the gestalt of this operation, two steps of level of authentication procedure and the significance of contents, i.e., the cryptographic key as decode information, are made into three kinds. The digital AV data transceiver system is constituted in drawing 10 by the transmitting unit 111 and the receiving unit 130 connected to it.
[0080] The transmitting unit 111 encryption means A and B112,113 to encipher the data A and B with which contents significance differs by respectively different cryptographic key Kco, and for encryption for example Kco for copy_never (contents which must not be recorded on a tape etc.), A Kco storage means 114 to memorize Kco for copy_once (contents which may be recorded only at once), and Kco for no_more_copy (contents which must not be copied any more), The object for copy_never called 'Exchange_Key', the object for copy_once, and a Kex generating means 115 to generate each cryptographic key Kex for no_more_copy which are

passed to the receiving unit 130, A Kex storage means 116 to memorize each of that generated Kex, and a seed generating means 117 to generate the kind used when computing the key Kco for encryption with a predetermined function, A seed storage means 118 to memorize the generated kind, and a Kco calculation means 119 to compute Kco by function Kco=f (a seed, Kex) using the kind from Kex and the seed storage means 118 from the Kex storage means 116, An authentication means 121 to perform authentication procedure to the receiving unit 130, A level judging means 122 to process judging level [finishing / authentication of the receiving unit 130] etc., It is constituted by a seed demand command response means 120 to answer to the seed demand from the receiving unit 130, and the digital interface (D-I/F) 123 which performs transmission and reception of data. Here, a part of seed demand command response means 120 and authentication means 121 constitute the decode information selection means.

[0081] Moreover, the digital interface 131 whose receiving unit 130 transmits and receives data (D-I/F), According to the significance of the contents of encryption digital AV data which received, on a demand level decision means 134 to determine the level of the authentication to demand, and its determined demand level An authentication means 133 to require authentication of the transmitting unit 111 and to acquire the required cryptographic key Kex, A Kex storage means 137 to memorize the acquired Kex, and a seed demand command issuance means 135 to publish the demand command of a seed and to acquire a seed from the transmitting unit 111, A Kco calculation means 136 to compute Kco by the same function Kco=f (a seed, Kex) as the transmitting unit 111 using Kex memorized by the acquired kind and the Kex storage means 137, It is constituted by decryption means 132 to decode encryption data by the computed Kco. Here, a part of seed demand command issuance means 135 and authentication means 133 constitute the decode information-requirements means.

[0082] Next, actuation of the digital AV data transceiver system of the gestalt of the above-mentioned implementation is explained, referring to a drawing.

[0083] In drawing 11 , first, in the receiving unit 130, the demand level decision means 134 determines the level of the authentication demanded based on the contents significance of received data, and passes the authentication means 133. The authentication means 133 gives an authentication demand to a transmitting unit through D-I/F131. Here, authentication of the highest level shall be required. In the transmitting unit 111, authentication processing is performed based on the authentication demand received through D-I/F123. About the approach of authentication, it can carry out by the approach explained with the gestalt of operation mentioned above, for example, and the shared common key Kab is obtained for a transmitting unit and a receiving unit at this time. Moreover, level [finishing / the authentication at this time] is passed to the level judging means 122.

[0084] Next, if authentication is completed and the advice is transmitted to the

receiving unit 130, since authentication level is the highest, the authentication means 133 will require Kex of all level from the transmitting unit 111. Here, they may be three kinds for the object for copy_never (Kex1), the object for copy_once (Kex2), and no_more_copy (Kex3) as level of Kex at high order.

[0085] In the transmitting unit 111, when it can pass with the judgment of whether the level judging means 122 can judge and pass carrier beam demand level based on attested level from the authentication means 121, it enciphers by Kab between which both own jointly Kex (it is Kex1, Kex2, and Kex3 at this time) with a demand, and transmits to the receiving unit 130 through the authentication means 121. In the receiving unit 130, it decodes by Kab in which self has Kab (Kex1, Kex2, Kex3) as which the authentication means 133 was enciphered, and memorizes for the Kex storage means 137.

[0086] On the other hand, Kex1 of each level which the Kex generating means 115 generated, i.e., Kex, and Kex2 and Kex3 are memorized by the Kex storage means 116, and the kind which the seed generating means 117 generated is memorized by the seed storage means 118. Moreover, using each Kex memorized by the Kex storage means 116 and the kind memorized by the seed storage means 118, the Kco calculation means 119 computed the object for copy_once, Kco for copy_never, i.e., the object, (Kco1) for each, (Kco2), and the object for no_more_copy (Kco3), and it has memorized for the Kco storage means 114. Furthermore, the encryption means A and B112,113 encipher digital AV data using Kco corresponding to the significance of the contents of each data, and transmit them to the receiving unit 130.

[0087] In the receiving unit 130, the seed demand command issuance means 135 transmits a seed demand command to the transmitting unit 111. If it does so, in the transmitting unit 111, the seed demand command response means 120 will transmit a seed to the ejection receiving unit 130 from the seed storage means 118. Here, because Kco for encryption is changed every moment, it is in the seed storage means 118 of drawing with a current kind and the following kind.

[0088] Next, in the receiving unit 130, the Kco calculation means 136 computes Kco using Kex corresponding to the level of the kind which the seed demand command issuance means 135 received from the transmitting unit 111, and the data which have been memorized for the Kex storage means and to decrypt with the same function (the transmitting unit and the receiving unit shall have this function beforehand, and the 3rd person shall not obtain it) as the transmitting unit 111. The decryption means 132 decodes the digital AV data enciphered using this computed Kco to the usual digital AV data. every first received when the data to be used changed or changed into the low data 2 (for example, sports program etc.) from the data 1 with a high contents significance (for example, film etc.) here -- since required Kex can be chosen from Naka of Kex and Kco can be computed and used, there is no need of also carrying out the demand of Kex, as well as a new authentication procedure.

[0089] Although the above-mentioned approach was the approach of acquiring all

available Kex(es) at once following authentication procedure, an approach as shown in drawing 12 may be used for it.
[0090] In drawing 12 , first, in the receiving unit 130, the demand level decision means 134 determines the level of the authentication demanded based on the contents significance of received data, and passes the authentication means 133. The authentication means 133 gives an authentication demand to a transmitting unit through D-I/F131. Here, authentication of the highest level shall be required. In the transmitting unit 111, authentication processing is performed based on the authentication demand received through D-I/F123. About the approach of authentication, it can carry out by the approach explained with the gestalt of operation mentioned above, for example, and the shared common key Kab is obtained for a transmitting unit and a receiving unit at this time. Moreover, level [finishing / the authentication at this time] is passed to the level judging means 122.
[0091] Next, if authentication is completed and the advice is transmitted to the receiving unit 130, the authentication means 133 will require Kex with the highest authentication level from the transmitting unit 111. Here, they may be three kinds for the object for copy_never (Kex1), the object for copy_once (Kex2), and no_more_copy (Kex3) as level of Kex at high order.
[0092] In the transmitting unit 111, when it can pass with the judgment of whether the level judging means 122 can judge and pass carrier beam demand level based on attested level from the authentication means 121, it enciphers by Kab between which both own jointly Kex (it is Kex1 at this time) with a demand, and transmits to the receiving unit 130 through the authentication means 121. In the receiving unit 130, it decodes by Kab in which self has Kab (Kex1) as which the authentication means 133 was enciphered, and memorizes for the Kex storage means 137.
[0093] Next, in the receiving unit 130, the seed demand command issuance means 135 transmits a seed demand command to the transmitting unit 111. If it does so, in the transmitting unit 111, the seed demand command response means 120 will transmit a seed to the ejection receiving unit 130 from the seed storage means 118.
[0094] The kind which the seed demand command issuance means 135 received from the transmitting unit 111 in the receiving unit 130 which received the seed, Kex (Kex1) corresponding to the level of the data which have been memorized for the Kex storage means and to decrypt is used. The Kco calculation means 136 Kco (Kco1) is computed with the same function (the transmitting unit and the receiving unit shall have this function beforehand, and the 3rd person shall not obtain it) as the transmitting unit 111. The decryption means 132 is this computed Kco1. The digital AV data used and enciphered are decoded to the usual digital AV data. Here, when the data to be used change or change into the low data 2 from the data 1 with a high contents significance, another Kex (drawing Kex2) is required from the transmitting unit 111.
[0095] In the transmitting unit 111, the level of Kex as which the level judging means

122 was required through the authentication means 121 is judged based on level [finishing / authentication], and if it is the demand of attested level and level lower than an EQC or it, demanded Kex (Kex2) will be enciphered by Kab, and it will transmit to the receiving unit 130.

[0096] When the receiving unit 130 performs the first authentication demand and authentication is completed here Memorize level [finishing / the authentication] (it is easy to be the thing of the highest level among level [finishing / authentication]), and the demand of Kex from next time is received. As long as it judges with the authentication means 133 and is available in whether Kex for which it asks from level [finishing / the memorized authentication] is available without authentication, you may make it require Kex. At this time, when it cannot obtain, what is necessary is just made to attest still newer high level. therefore, the past attested level and the EQC the demand level determined with the demand level decision means 134 based on the contents significance of digital AV data is remembered to be -- or when it is the level not more than it, desired Kex is required from the authentication means 133.

[0097] Moreover, about the transmitting unit 111 side, there is no authentication demand and there is a demand of Kex, and when demanded Kex is judged as transmission being impossible, it is good also as an approach of notifying the information on a purport being attested new to the receiving unit 130 side.

[0098] In the receiving unit 130, the authentication means 133 decodes Kab (Kex2), and it memorizes for the Kex storage means 137, and the Kco calculation means 136 computes Kco2 using the Kex2 and kind, and decodes data. Since according to this approach there will be no need of newly performing authentication procedure when acquiring Kex of that level and the level not more than an EQC or it if authentication on the level which has 1 time has ended, the count of the authentication procedure which time amount requires will be decreased.

[0099] By the way, by the approach of performing authentication procedure each time, when many receiving units are connected, the frequency of an authentication demand increases to use like before AV data with which the significance of contents differs. However, in the thing using the isochronous data communication and asynchronous data communication like for example, IEEE1394BUS specification, since the communication link for an authentication demand is carrying out using a part of band originally used for the communication band of data, it is not desirable. [of the frequency of the authentication demand which time amount requires increasing] Therefore, according to the gestalt of this operation, even if the number of a receiving unit increases, since it can be fundamentally managed with one authentication procedure about 1 receiving unit, the inconvenience by authentication demand does not arise.

[0100] In addition, with the gestalt of implementation of the above fifth, although level of authentication procedure was made into two steps, it is not limited to this.

[0101] Moreover, with the gestalt of implementation of the above fifth, although level

of the significance of contents was made into three kinds, it is not limited to this. For example, the level of copy_free (contents which may be recorded any number of times) is applied, and it is good also as four kinds, and good also as a class beyond it.
[0102] Moreover, although considered as the configuration realized by the approach of computing the key for encryption with a function using a seed and a cryptographic key with the gestalt of implementation of the above fifth, you may apply to the configuration using the approach explained with the gestalt of operation of not only this but others.
[0103] Moreover, although the class of Kex which looks at and requires the significance of the data under reception is determined with the gestalt of implementation of the above fifth, all Kex(es) that he may receive beforehand may be acquired.
[0104] Moreover, after attesting, although [the gestalt of implementation of the above fifth / a receiving unit] Kex is required, it is not limited to this. For example, when carrying out an authentication demand, and it applies for the class of Kex which he wants to receive simultaneously to a transmitting unit and authentication is completed, Kex as which the transmitting unit was required automatically may be transmitted to a receiving unit.
[0105] Moreover, although it was the approach of changing a cryptographic key according to the significance of data, you may make it change a cryptographic key with the gestalt of implementation of the above fifth according to the class of not only this but data etc. In that case, it is necessary to make the level of authentication, and the class (namely, cryptographic key) of data correspond.
[0106] Next, the gestalt of operation of the sixth of this invention is explained.
[0107] Drawing 13 is a schematic diagram about the gestalt of operation of the sixth of this invention. The digital AV data receiving unit 160 equipped with both the functions of the digital AV data receiving unit 150 only with a Rest authentication function and Full authentication, and Rest authentication shall be connected to the digital AV data transmitting unit 140 which the gestalt of this operation equipped with Full authentication and a Restricted authentication (it is hereafter called Rest authentication for short) function. Here, Full authentication shall be the authentication approach of a high level using a public key and a private key, and Rest authentication shall show the usual authentication approach of having used the common key.
[0108] In drawing 13 the digital AV data transmitting unit 140 As an encryption means 141 to encipher data, a Full authentication storing means 143 to store the rule for Full authentication, a Rest authentication storing means 142 to store the rule for Rest authentication, and management criteria ** CRL () [Certification] RevocationList : It responds to the selection result of a CRL storing means 144 to store the inaccurate equipment list for eliminating an inaccurate device, a transmitting-side authentication selection means 147 to choose an authentication rule in response to the authentication demand from a receiving unit, and its transmitting-side authentication

selection means 147. By the change means 148 which changes Full authentication and Rest authentication, and the authentication rule changed and chosen Encryption data, an authentication demand, etc. consist of D-I/F(digital interface) 145 which exchange information between the authentication means 146 which attests between receiving units, and the receiving unit. CRL is added to input data and updated by the new content at any time.

[0109] On the other hand, the digital AV data receiving unit 150 consists of D-I/F151 which exchanges information, such as encryption data and an authentication demand, between transmitting units, a decryption means 152 to decrypt the encryption data received from the transmitting unit, an authentication demand means 153 to perform an authentication demand to a transmitting unit, and an authentication means 154 that attests by the Rest authentication rule.

[0110] Moreover, the digital AV data receiving unit 160 As opposed to D-I/F161 which exchanges information, such as encryption data and an authentication demand, between transmitting units, a decryption means 162 to decrypt the encryption data received from the transmitting unit, and a transmitting unit With the directions from an authentication demand means 163 to perform an authentication demand, a Full authentication storing means 166 to store the rule for Full authentication, a Rest authentication storing means 165 to store the rule for Rest authentication, and the authentication demand means 163 It consists of a change means 167 which changes an authentication rule, and an authentication means 164 which attests by the authentication rule changed and chosen.

[0111] Next, it explains, referring to a drawing about actuation of the gestalt of the above-mentioned implementation.

[0112] First, although the above-mentioned CRL is sent from a management pin center,large, in order to receive, it uses the function of Full authentication. Therefore, CRL cannot come to hand by the device only with a Rest authentication function. Therefore, the device side only with a Rest authentication function cannot perform device abatement by the CRL check. Here, the procedure which used the CRL check is explained about the case where both a transmitting unit and a receiving unit have Full authentication and a Rest authentication function.

[0113] Drawing 15 adds a CRL check to the authentication approach by the public key and private key which were shown in drawing 4 .

[0114] In drawing 15 , to a transmitting side, IDa for discernment of the unit and the signature A to the IDa shall be sent from a management pin center,large (license device), and IDb for discernment of the unit and the signature B to the IDb shall be sent to a receiving side from the management pin center,large at it. Moreover, a receiving side has a private key Sb and a public key Pb in this case. Moreover, a transmitting side has a private key Sa and a public key Pa.

[0115] First, a receiving side generates a random number B at step 41. A receiving side sends the cipher Sb (B) which enciphered IDb and Signature B which are the

recognition number of self, and the random number B with its private key Sb to a transmitting side. A transmitting side is searched from the recognition number IDb of a receiving side, and receives the public key Pb of a receiving side. Cipher Sb (B) is decrypted with the public key Pb which came to hand at step 49. As a result, a random number B is obtained like step 50. Furthermore, a transmitting side is step 51 and performs a CRL check to IDb of a receiving side. That is, it investigates whether there is any IDb in CRL, and if there is nothing, a random number A will be generated at step 52. Authentication is stopped noting that it will be an inaccurate device, if it is in CRL. At step 52, random numbers A and B are enciphered with the private key Sa of a transmitting side, and Cipher Sa (A, B) is created. A transmitting side transmits Cipher Sa (A, B) and the recognition number IDa of self to a receiving side. A receiving side searches the recognition number IDa of Cipher Sa (A, B) and a transmitting side from reception and the recognition number IDa of a transmitting side, receives the public key Pa of a transmitting side, and decrypts Cipher Sa (A, B) by Pa like step 42. Here, a receiving side understands that the random number B sent to the receiving side at step 41 and the completely same random number B are obtained from Cipher Sa (A, B), and neither forgery nor an alteration is performed. If said two random numbers differ, it turns out that it turns out that forgery and an alteration were performed and there is an inaccurate partner. However, public keys Pa and Pb shall come to hand no longer only to a just person in this case. Next, like step 43, a receiving side enciphers a random number A with the private key Sb of a receiving side, and creates Cipher Sb (A). Sb (A) is sent to a transmitting side and decrypts Cipher Sb (A) like step 53 with the public key Pb of a receiving side which it already has by the transmitting side. If the random number A and the random number A decrypted at step 53 generated at step 52 are completely the same, a transmitting side understands that neither forgery nor an alteration is performed. If said two random numbers differ, it turns out that it turns out that forgery and an alteration were performed and there is an inaccurate partner.

[0116] On the other hand, a receiving side performs a CRL check to IDa of a transmitting side at step 44. And if IDa is in CRL, authentication will be stopped, and if there is nothing, it will move to the following step. Now, supposing, as for the random numbers A and B which the result of the CRL check by the transmitting side and the receiving side is normal, and exchanged by the receiving side and the transmitting side, neither forgery nor an alteration is performed, random numbers A and B are random numbers of secrecy at the 3rd person other than a receiving side and a transmitting side. Then, by the transmitting side, Key Kab is created like step 54 using random numbers A and B. Similarly Key Kab is created using random numbers A and B by the receiving side like step 45. Said two Kab(s) are the same and completely serve as a common key. Next, Key Kex is created like step 55 by the transmitting side. This is enciphered with the common key Kab, Cipher Kab (Kex) is created, and it sends to a receiving side. The key Kex which the receiving side decrypted Cipher Kab

(Kex) with the common key Kab like step 46, and obtained Kex, consequently the receiving side obtained, and the key Kex in a transmitting side are completely the same, and turn into a common key. Next, Key Kco is created like step 56 by the transmitting side. It is enciphered with the common key Kex and Key Kco is sent to a receiving side as a cipher Kex (Kco). In a receiving side, like step 47, Cipher Kex (Kco) is decrypted with the common key Kex, and Kco is obtained like step 48. The key Kco in a transmitting side and Kco in a receiving side are completely the same, and serve as a common key. The above is the work-piece key Kco obtained in process of authentication by the public key and the private key.

[0117] In the above-mentioned explanation, although the CRL check was performed before generating of the random number A of step 52, as long as it is after IDb reception, you may carry out anywhere. A specification top is performed after step 54 which creates KAB.

[0118] Next, a receiving side explains the case of only a Rest authentication function. When performing authentication with this common key, an approach which was mentioned above cannot be used. Then, the signature created by the receiving side using ID for CRL to the unit and its ID is given, and the approach of using CRL by the transmitting side is used.

[0119] In drawing 14 , IDb of a receiving unit and Signature B are given to a receiving side from a management pin center,large, and a transmitting side and a receiving side have the common key S in it. In addition, this common key is given only to the just person. First, two random numbers A1 and A2 are generated like step 30 in a receiving side, it enciphers with the common key S, Cipher S (A1A2) is created, and it sends to a transmitting side with IDb and Signature B. In a transmitting side, Cipher S (A1A2) is decrypted with the common key S like step 35. And a CRL check is performed to IDb of a receiving side. Moreover, Signature B is checked. Authentication is stopped when either a CRL check or the check of Signature B has abnormalities at this time. If both of the result of a CRL check and the check of Signature B are normal, a random number A1 and a random number A2 will be obtained like step 37. A transmitting side sends a random number A2 to a receiving side. A receiving side will have two random numbers A1 and A2 like step 31. If the random number A2 received from the transmitting side at step 31 is completely the same as the random number A2 generated at step 30, it turns out that neither forgery nor an alteration is performed by the transmitting side. If the two above-mentioned random numbers differ, it will mean that forgery and an alteration were performed and authentication will go wrong. Next, like step 38, a transmitting side generates a random number B1 and B-2, enciphers and sends Cipher S (B1 B-2) to a receiving side. A receiving side decrypts Cipher S (B1 B-2) using the common key S like step 32. Then, a random number B1 and B-2 are obtained like step 33. A receiving side sends random-number B-2 to a transmitting side. A transmitting side will have a random number B1 and B-2 like step 39. If random-number B-2 received from the

receiving side at step 39 is the same as random-number B-2 generated at step 38, it will turn out that neither forgery nor an alteration is performed to the receiving side, and authentication will be successful. If the two above-mentioned random numbers differ, it means that forgery and an alteration were performed and authentication is failure.

[0120] Here, supposing authentication was successful, a random number A1 and a random number B1 are random numbers of secrecy at the 3rd person other than a transmitting side and a receiving side. In a transmitting side, Key Kco is created like step 40 from IDb and a random number A1, and a random number B1. On the other hand by the receiving side, Key Kco is created like step 34 from IDb and a random number A1, and a random number B1. The key Kco in a transmitting side and the key Kco in a receiving side are completely the same, and are a common key. The above is the work-piece key Kco obtained in process of authentication with a common key. According to this approach, since IDb and Signature B correspond, even if IDb is stolen and the CRL check in a transmitting side passes, an unauthorized use can be prevented with the check by Signature B.

[0121] Here, ID for CRL uses a 40-bit device ID. By this, it will not be concerned with Full authentication and Rest authentication, but all 1394CP devices will have a 40-bit device ID.

[0122] In addition, in the above-mentioned explanation, although creation of a signature in a management pin center,large was created using ID, a management pin center,large decides this ID to be arbitration. Furthermore, in order to raise safety, when manufacturing a device, NUID which is the identifier of the device proper beforehand embedded for every device is used. That is, in case it applies for a receiving side to a management pin center,large, it tells NUID of the device, and a management pin center,large creates a signature using the NUID and ID for CRL, and gives ID for CRL, and a signature to a receiving side.

[0123] Moreover, although the class of authentication rule was made into two kinds, Full and Rest, the class of authentication rule is not limited to this, and even if it is three or more kinds, it is applicable with the gestalt of the above-mentioned implementation, in the case of the configuration in which a receiving side cannot have CRL like the above-mentioned.

[0124] Moreover, each component of this invention is not cared about, whether the hard circuit of the dedication which realizes each function, a device, etc. realize or it realizes by software using a computer.

[0125] Moreover, when a computer realizes this invention, the medium which stored the program for realizing all or a part of functions of each of those components also belongs to this invention.

[0126]

[Effect of the Invention] So that clearly from the place explained above this invention Authentication of unimportant data does not take much time amount, but it is related

with important data. When the authentication changes strictness required for authentication to forgery or an alteration with a unit strongly again, in consideration of the classification of the authentication approach which the importance of data and a partner's equipment have etc., a unit, a system, etc. which can transmit and receive data by the suitable authentication approach can be offered.

[0127] Moreover, this invention has the advantage that the count of authentication can be decreased, when acquiring two or more kinds of decode information according to the significance of contents.

[0128] Moreover, even if this invention is a receiver without an abatement function, it becomes possible [eliminating a device by the transmitting side].

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The schematic diagram about the gestalt of operation of the first of this invention

[Drawing 2] The schematic diagram showing the conventional technique

[Drawing 3] The schematic diagram showing the conventional technique

[Drawing 4] The block diagram concerning the authentication approach among the gestalten of operation of this invention

[Drawing 5] The block diagram concerning the authentication approach among the gestalten of operation of this invention

[Drawing 6] The schematic diagram about the gestalt of operation of the second of this invention

[Drawing 7] The schematic diagram about the gestalt of operation of the third of this invention

[Drawing 8] The schematic diagram about the gestalt of operation of the fourth of this invention

[Drawing 9] The schematic diagram about the gestalt of operation of the fourth of this invention

[Drawing 10] The schematic diagram about the gestalt of operation of the fifth of this invention

[Drawing 11] Drawing showing an example of the procedure approach in the gestalt of this fifth operation

[Drawing 12] Drawing showing another example of the procedure approach in the gestalt of this fifth operation

[Drawing 13] The schematic diagram about the gestalt of operation of the sixth of this invention

[Drawing 14] Drawing showing an example of the procedure approach in the gestalt of this sixth operation

[Drawing 15] Drawing showing an example of the procedure approach in the case of performing a CRL check by both the transmitting side and the receiving side

[Description of Notations]

1 STB
3 Data Importance Judging Means
5 Transmitting-Side Two or More Authentication Rule Storing Means
6 Transmitting-Side Authentication Selection Means
7 Transmitting-Side Authentication Means
9 TV
13 Receiving-Side Authentication Means
14 Receiving-Side Two or More Authentication Rule Storing Means
15 Receiving-Side Authentication Selection Means
18 STB
19 Authentication Means
20 Public Key/Private Key
23 TV
25 Authentication Means
26 Public Key/Private Key
28 STB
29 Authentication Means
30 Common Key
33 TV
35 Authentication Means
36 Common Key
38 STB
41 Transmitting-Side Two or More Authentication Rule Storing Means
42 Unit Authentication Rule Information Receiving Means
43 Transmitting-Side Authentication Means
45 VTR
48 Authentication Demand Means
49 Receiving-Side Authentication Rule Storing Means
50 Authentication Rule Information Transmitting Means
51 Receiving-Side Authentication Means
55 Transmitting-Side Authentication Rule Ejection Means
56 STB
57 Data Importance Judging Means
58 Transmitting-Side Authentication Rule Ejection Means
59 Transmitting-Side Authentication Selection Means
60 Unit Authentication Rule Information Receiving Means

61 Transmitting-Side Authentication Means
63 Transmitting-Side Two or More Authentication Rule Storing Means
65 TV
67 Authentication Demand Means
68 Receiving-Side Two or More Authentication Rule Storing Means
69 Receiving-Side Authentication Selection Means
70 Receiving-Side Authentication Means
72 VTR
74 Authentication Demand Means
75 Receiving-Side Authentication Rule Storing Means
76 Authentication Rule Information Transmitting Means
77 Receiving-Side Authentication Means
86 Data Importance Judging Means
87 Management-Criteria Reference Decision Means
88 Management-Criteria Storing Means
89 Authentication Decision Means
90 Authentication Means
92 TV
93 STB
94 STB
95 Management-Criteria Reference Decision Means
96 Management-Criteria Storing Means
97 Authentication Decision Means
98 Authentication Means
100 VTR
144 CRL Storing Means

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－59323
（P2000－59323A）
(43)公開日　平成12年２月25日(2000.2.25)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*（参考）
Ｈ０４Ｈ　1/00		Ｈ０４Ｈ　1/00	Ｆ	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	
9/10			６２１	
29/08		13/00	３０７Ｚ	
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	Ｚ	

審査請求　未請求　請求項の数43　ＯＬ　（全 28 頁）

(21)出願番号　特願平10－224825

(22)出願日　平成10年８月７日(1998.8.7)

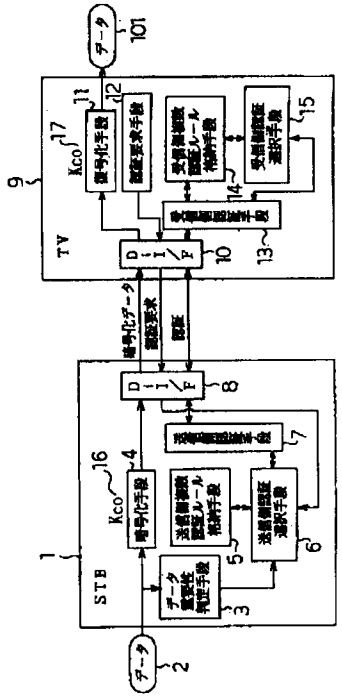
(31)優先権主張番号　特願平10－31847
(32)優先日　平成10年２月13日(1998.2.13)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平10－151586
(32)優先日　平成10年６月１日(1998.6.1)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　西村　拓也
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　飯塚　裕之
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100092794
弁理士　松田　正道

最終頁に続く

(54)【発明の名称】　デジタルＡＶデータ送信ユニット、デジタルＡＶデータ受信ユニット及び、デジタルＡＶデータ送受信システム、媒体

(57)【要約】
【課題】　重要でないデータの認証に多くの時間を要したり、重要なデータであるにもかかわらずその認証が偽造や改竄に弱い。また、ユニットによって認証に必要な厳密さが異なる。
【解決手段】　データ２の重要度を判定するデータ重要性判定手段３、その判定結果に基き送信側複数認証ルール格納手段５から一種類のルールを選択する送信側認証選択手段６及び、その選択された認証ルールに基づき認証を行う送信側認証手段７を有するＳＴＢ１と、認証要求を行う認証要求手段１２、送信側で選択された認証ルールと同じ認証ルールを受信側複数認証ルール格納手段１４から選択する受信側認証選択手段１５及び、その選択された認証ルールに基づき認証を行う受信側認証手段１３を有するＴＶ９とを備える。



【特許請求の範囲】

【請求項１】　デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニット。

【請求項２】　デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶデータ送信ユニットを通信の対象とし、

前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ受信ユニット。

【請求項３】　デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、

前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルＡＶデータ受信ユニットとを備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項４】　デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、所定の管理基準を格納した管理基準格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記管理基準格納手段の前記管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って前記管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニット。

【請求項５】　前記送信ユニットは前記受信ユニットの各機能を有し、前記受信ユニットは前記送信ユニットの各機能を有することを特徴とする請求項３記載のデジタルAVデータ送受信システム。

【請求項６】　前記受信ユニットの機能を有する送信ユニット、あるいは前記送信ユニットの機能を有する受信ユニットが三つ以上互いに接続され、デジタルAVデータを互いにやりとりできることを特徴とする請求項５記載のデジタルAVデータ送受信システム。

【請求項７】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶ送信ユニット。

【請求項８】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットを通信の対象とし、

前記認証の要求を行う認証要求手段と、自らの一種類の前記認証ルールを格納する受信側認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ受信ユニット。

【請求項９】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ル

ール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、
前記認証の要求を行う認証要求手段と、自らの一種類の前記認証ルールを格納する受信側認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段を少なくとも有するデジタルＡＶデータ受信ユニットと、を備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項１０】　所定の管理基準を格納した管理基準格納手段と、デジタルＡＶデータ受信ユニットから認証要求を受けて、そのデジタルＡＶデータ受信ユニットの種類又は重要度に応じて、前記管理基準格納手段の前記管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って前記管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたことを特徴とするデジタルＡＶ送信ユニット。

【請求項１１】　前記管理基準は、不正な、あるいは正当なデジタルＡＶデータ受信ユニットを識別できる基準リスト（ＣＲＬ）であることを特徴とする請求項４又は１０に記載のデジタルＡＶ送信ユニット。

【請求項１２】前記送信ユニットに、前記受信ユニットが二つ以上接続され、前記送信ユニットとの間で、デジタルＡＶデータをやりとりできることを特徴とする請求項９記載のデジタルＡＶデータ送受信システム。

【請求項１３】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記単一認証デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、前記送信側認証選択手段又は前記送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニット。

【請求項１４】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記単一認証デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、前記送信側認証選択手段又は前記送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも有するデジタルＡＶデータ送信ユニットと、
前記認証の要求を行う認証要求手段と、前記送信側認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有する複数認証デジタルＡＶデータ受信ユニットと、
認証の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側単一認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記デジタルＡＶデータ送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段を少なくとも有する単一認証デジタルＡＶデータ受信ユニットと、を備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項１５】前記複数認証デジタルＡＶデータ受信ユニットは前記デジタルＡＶデータ送信ユニットの各機能を有し、前記デジタルＡＶデータ送信ユニットは前記複数認証デジタルＡＶデータ受信ユニットの各機能を有することを特徴とする請求項１４記載のデジタルＡＶデータ送受信システム。

【請求項１６】前記複数認証デジタルＡＶデータ受信ユニットの各機能を有するデジタルＡＶデータ送信ユニット、あるいは前記デジタルＡＶデータ送信ユニットの機能を有する複数認証デジタルＡＶデータ受信ユニットが二つ以上互いに接続され、且つ、前記単一認証デジタルＡＶデータ受信ユニットが二つ以上接続され、デジタルＡＶデータを互いにやりとりできることを特徴とする請求項１５記載のデジタルＡＶデータ送受信システム。

【請求項１７】　デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、前記暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、前記受信ユニットからの、前記暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、前記判定済みの認証レベルと同等及びそれ以下のレベルの前記解読情報を、前記受信ユニットに送信

する解読情報選択手段とを備えたことを特徴とする送信ユニット。

【請求項１８】　データの重要度に応じた複数のレベルで暗号化されたデジタルＡＶデータを送信する送信ユニットから受信する暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を前記送信ユニットに要求する認証手段と、前記認証レベルと同等及びそれ以下のレベルの前記暗号化データに対する解読情報を、前記送信ユニットに要求する解読情報要求手段とを備えたことを特徴とする受信ユニット。

【請求項１９】　デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、前記暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、前記受信ユニットからの、前記暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、前記判定済みの認証レベルと同等及びそれ以下のレベルの前記解読情報を、前記受信ユニットに送信する解読情報選択手段とを有する送信ユニットと、
その送信ユニットから受信する暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を前記送信ユニットに要求する認証手段と、前記認証レベルと同等及びそれ以下のレベルの解読情報を、前記送信ユニットに要求する解読情報要求手段とを有する受信ユニットとを備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項２０】　デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、前記暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、前記受信ユニットからの、前記暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、前記判定済みの認証レベルと同等またはそれ以下のレベルの解読情報を前記受信ユニットに送信する解読情報選択手段とを備え、前記解読情報選択手段は、次に前記受信ユニットから解読情報の要求があった時に、その要求が前記判定済みの認証レベルと同等あるいはそれ以下のレベルの前記解読情報の場合は、前記認証手続きを行わずに要求された解読情報を前記受信ユニットに送信することを特徴とする送信ユニット。

【請求項２１】　データの重要度に応じた複数のレベルで暗号化されたデジタルＡＶデータを送信する送信ユニットから受信する暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を前記送信ユニットに要求する認証手段と、前記認証レベルと同等またはそれ以下のレベルの前記暗号化データに対する解読情報を前記送信ユニットに要求する解読情報要求手段とを備え、前記解読情報要求手段は、前記認証のレベルと同等あるいはそれ以下のレベルの解読情報を前記送信ユニットに要求する時は、前記認証要求を行わずに、前記解読情報の要求を行うことを特徴とする受信ユニット。

【請求項２２】　デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、前記暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、前記受信ユニットからの、前記暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、前記判定済みの認証レベルと同等またはそれ以下のレベルの解読情報を前記受信ユニットに送信する解読情報選択手段とを有し、前記解読情報選択手段は、次に前記受信ユニットから解読情報の要求があった時に、その要求が前記判定済みの認証レベルと同等あるいはそれ以下のレベルの前記解読情報の場合は、前記認証手続きを行わずに要求された解読情報を前記受信ユニットに送信する送信ユニットと、
その送信ユニットから受信する暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を前記送信ユニットに要求する認証手段と、前記認証レベルと同等またはそれ以下のレベルの解読情報を前記送信ユニットに要求する解読情報要求手段とを備え、前記解読情報要求手段は、前記認証のレベルと同等あるいはそれ以下のレベルの解読情報を前記送信ユニットに要求する時は、前記認証要求を行わずに、前記解読情報の要求を行う受信ユニットとを備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項２３】　受信側ユニットから送られてきた認証要求について、認証を行い、又、その認証のレベルを判定し、そのレベルと同等な認証方法及びそれより低いレベルの認証方法に対応する暗号化方法のそれぞれの解読情報を、前記受信側ユニットからの解読情報の要求に応じて、前記受信側ユニットへ送信することを特徴とするデジタルＡＶデータ送信方法。

【請求項２４】　受信側ユニットから送られてきた解読情報要求について、その要求された解読情報に対応する認証のレベルを判定し、そのレベルと前記受信側ユニットとの間で過去に実行した認証のレベルとを比較し、前記判定された認証のレベルが過去の認証のレベルと同等もしくはより低いレベルの場合は、前記受信側ユニットから前記要求された解読情報を送信することを特徴とするデジタルＡＶデータ送信方法。

【請求項２５】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、その送信側複数認証ルール格納手段から１種類の認証ルールを選択する送信側認

証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶデータ送信ユニットであって、
認証の要求を行い、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段から１種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルＡＶデータ受信ユニットまたは、前記送信ユニットにおける認証ルールの選択は、データの重要度の判定結果に基づいて行われ、前記重要度の判定を行ったユニットが重要度の判定を行わないユニットに前記選択した認証ルールについての情報を送り、前記重要度の判定を行わないユニットは、その情報に基づいて、同じ認証ルールを選択することを特徴とするデジタルＡＶデータ送信ユニット。

【請求項２６】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段から１種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルＡＶデータ送信ユニットに対して、認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記受信側複数認証ルール格納手段から１種類の認証ルールを選択する受信側認証選択手段と、その選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたデジタルＡＶデータ受信ユニットであって、前記送信ユニットまたは受信ユニットにおける認証ルールの選択は、データの重要度の判定結果に基づいて行われ、前記重要度の判定を行ったユニットが重要度の判定を行わないユニットに前記選択した認証ルールについての情報を送り、前記重要度の判定を行わないユニットは、その情報に基づいて、同じ認証ルールを選択することを特徴とするデジタルＡＶデータ受信ユニット。

【請求項２７】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、その送信側複数認証ルール格納手段から１種類の認証ルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、
前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記受信側複数認証ルール格納手段から１種類の認証ルールを選択する受信側認証選択手段と、その選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルＡＶデータ受信ユニットとを備え、前記送信ユニットまたは受信ユニットにおける認証ルールの選択は、データの重要度の判定結果に基づいて行われ、前記重要度の判定を行ったユニットが重要度の判定を行わないユニットに前記選択した認証ルールについての情報を送り、前記重要度の判定を行わないユニットは、その情報に基づいて、同じ認証ルールを選択することを特徴とするデジタルＡＶデータ送受信システム。

【請求項２８】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証の要求を行い、デジタルＡＶデータの重要度を判定してその判定結果に基づいて、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段から一種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルＡＶデータ受信ユニットで選択される前記認証ルールと同じルールを、前記送信側複数認証ルール格納手段から選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニット。

【請求項２９】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段から受信側で選択される所定の認証ルールと同じ認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルＡＶデータ送信ユニットに対して、認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、そのデータ重要性判定手段の判定結果に基づいて、前記受信側複数認証ルール格納手段から一種類の認証ルールを選択する受信側認証選択手段と、その選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ受信ユニット。

【請求項３０】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、その送信側複数認証ルール格納手段から受信側で選択される所定の認証ルールと同じルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、
前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、そのデータ重要性判定手段の判定結果に基づいて、前記受信側複数認証ルール格納手段から一種類のルールを選択する受信側認証選択手段と、その選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルＡＶデータ受信ユニットとを備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項３１】　複数種類の認証ルールから１種類の認証ルールを選択して認証を行う認証手段と、受信ユニットに対する所定の管理基準を格納した管理基準格納手段と、前記受信ユニットからの認証要求を受け、前記格納されている管理基準を参照することにより認証するか否

かを判定する認証判定手段とを備えたデジタルＡＶデータ送信ユニットであって、前記認証要求を行う受信ユニットが、前記管理基準を持てない重要度の低い認証ルールのみで認証する機能しか有しない場合に、前記受信ユニットは、外部の管理センターからその受信ユニットに対応する前記管理基準用の識別情報が付与されるものであり、前記送信ユニットの認証判定手段は、前記認証要求の際に前記識別情報を受け取り、その識別情報が不可となった場合に、前記認証を取りやめることを特徴とするデジタルＡＶデータ送信ユニット。

【請求項３２】　受信ユニットからの認証要求を受け、管理基準格納手段に格納されている受信ユニットに対する所定の管理基準を参照することにより認証するか否かを判定する認証判定手段を有するデジタルＡＶデータ送信ユニットに対し、前記認証要求を行う認証要求手段と、前記管理基準を持てない重要度の低い認証ルールのみで認証する認証手段とを備え、外部の管理センターから受信ユニット自身に対応する前記管理基準用の識別情報が付与されるデジタルＡＶデータ受信ユニットであって、前記送信ユニットの認証判定手段は、前記認証要求の際に前記識別情報を受け取り、その識別情報が不可となった場合に、前記認証を取りやめることを特徴とするデジタルＡＶデータ受信ユニット。

【請求項３３】　複数種類の認証ルールから１種類の認証ルールを選択して認証を行う認証手段と、受信ユニットに対する所定の管理基準を格納した管理基準格納手段と、前記受信ユニットからの認証要求を受け、前記格納されている管理基準を参照することにより認証するか否かを判定する認証判定手段とを有するデジタルＡＶデータ送信ユニットと、その送信ユニットに対し、前記認証要求を行う認証要求手段と、前記管理基準を持てない重要度の低い認証ルールのみで認証する認証手段とを有し、外部の管理センターから受信ユニット自身に対応する前記管理基準用の識別情報が付与されるデジタルＡＶデータ受信ユニットとを備え、前記送信ユニットの認証判定手段は、前記認証要求の際に前記識別情報を受け取り、その識別情報が不可となった場合に、前記認証を取りやめることを特徴とするデジタルＡＶデータ送受信システム。

【請求項３４】　前記所定の管理基準は、不正な、あるいは正当なデジタルＡＶデータ受信ユニットを識別できる基準リストであり、前記識別情報が、前記受信ユニットに対応する前記管理基準用のＩＤおよびそのＩＤに対する署名であることを特徴とする請求項３１記載のデジタルＡＶデータ送信ユニット。

【請求項３５】　前記認証判定手段は、前記ＩＤ及び署名の少なくと一方が不可となった場合に、前記認証を取りやめることを特徴とする請求項３４記載のデジタルＡＶデータ送信ユニット。

【請求項３６】　前記署名は、受信ユニットそれぞれにあらかじめ固有に付加されている識別ＩＤを利用して作成されるものであることを特徴とする請求項３４、または３５記載のデジタルＡＶデータ送信ユニット。

【請求項３７】　前記所定の管理基準は、不正な、あるいは正当なデジタルＡＶデータ受信ユニットを識別できる基準リストであり、前記識別情報が、前記受信ユニットに対応する前記管理基準用のＩＤおよびそのＩＤに対する署名であることを特徴とする請求項３２記載のデジタルＡＶデータ受信ユニット。

【請求項３８】　前記認証判定手段は、前記ＩＤ及び署名の少なくと一方が不可となった場合に、前記認証を取りやめることを特徴とする請求項３７記載のデジタルＡＶデータ受信ユニット。

【請求項３９】　前記署名は、受信ユニットそれぞれにあらかじめ固有に付加されている識別ＩＤを利用して作成されるものであることを特徴とする請求項３７、または３８記載のデジタルＡＶデータ受信ユニット。

【請求項４０】　前記所定の管理基準は、不正な、あるいは正当なデジタルＡＶデータ受信ユニットを識別できる基準リストであり、前記識別情報が、前記受信ユニットに対応する前記管理基準用のＩＤおよびそのＩＤに対する署名であることを特徴とする請求項３３記載のデジタルＡＶデータ送受信システム。

【請求項４１】　前記認証判定手段は、前記ＩＤ及び署名の少なくと一方が不可となった場合に、前記認証を取りやめることを特徴とする請求項４０記載のデジタルＡＶデータ送受信システム。

【請求項４２】　前記署名は、受信ユニットそれぞれにあらかじめ固有に付加されている識別ＩＤを利用して作成されるものであることを特徴とする請求項４０、または４１記載のデジタルＡＶデータ送受信システム。

【請求項４３】　請求項１～４２のいずれかに記載のユニット又はシステムもしくは送信方法が有する各構成要素もしくはステップが持つ機能の全部又は一部を実現するためのプログラムを格納したことを特徴とする媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＡＶ装置間において認証を行う機能を持つＡＶシステムに関するものである。

【０００２】

【従来の技術】従来のＡＶ装置間において認証を行うシステムについて図２と図３を用いて説明する。

【０００３】まず、図２において、デジタルＡＶデータ送信ユニットＳＴＢ１８は、公開鍵と秘密鍵２０、認証手段１９、デジタルインターフェースＤ－Ｉ／Ｆ２２、暗号化手段１９を備えている。その公開鍵と秘密鍵２０は、認証手段１９を介して、デジタルインターフェースＤ－Ｉ／Ｆ２２に接続している。また、暗号化手段１９は、公開鍵と秘密鍵２０を参照することが出来、デジタ

ルインターフェース２２に接続している。デジタルＡＶデータ受信ユニットＴＶ２３も公開鍵と秘密鍵２６、認証手段２５、デジタルインターフェースＤ－Ｉ／Ｆ２４、復号化手段２７を具備している。その公開鍵と秘密鍵２６は認証手段２５を介してデジタルインターフェースＤ－Ｉ／Ｆ２４に接続している。また、復号化手段２７は公開鍵と秘密鍵２６を参照することが出来、デジタルインターフェースＤ－Ｉ／Ｆ２４に接続している。さらにデジタルインターフェースＤ－Ｉ／Ｆ２２とデジタルインターフェースＤ－Ｉ／Ｆ２４は互いにデータのやり取りが出来る構成となっている。

【０００４】次にデジタルＡＶデータ送信ユニットＳＴＢ１８とデジタルＡＶデータ受信ユニットＴＶ２３間の動作を説明する。まず、デジタルＡＶデータ受信ユニットＴＶ２３が認証要求を出す。するとデジタルインターフェースＤ－Ｉ／Ｆ２４を通してデジタルＡＶデータ送信ユニットＳＴＢ１８を構成するデジタルインターフェースＤ－Ｉ／Ｆ２２に認証要求が到達する。デジタルインターフェースＤ－Ｉ／Ｆ２２は認証要求を受けて認証手段１９にて、公開鍵と秘密鍵２０を参照して認証する。デジタルＡＶデータ送信ユニットＳＴＢ１８にて認証されれば、暗号化手段２１において、データが暗号化されて、デジタルインターフェースＤ－Ｉ／Ｆ２２を介して、暗号化したデータが送信される。これはデジタルインターフェースＤ－Ｉ／Ｆ２４を介して、公開鍵と秘密鍵２６を参照して、復号化手段２７で復号される。

【０００５】このようにすると、偽造や改竄に強い機能が実現出来る。しかし、公開鍵と秘密鍵を用いた認証は多くの時間を要する。ニュースのように、あまり重要でないデータの場合、不必要に認証に時間を取られることがある。またＶＴＲのようにコピー可能なデータしか受け取っては機器は、場合によってデジタルＡＶデータ受信ユニットが厳密な認証を要しないこともあり、そのような場合、時間の無駄が生じる。

【０００６】次に、図３において、デジタルＡＶ送信ユニットＳＴＢ２８は共通鍵３０、認証手段２９、デジタルインターフェースＤ－Ｉ／Ｆ３２、暗号化手段３１を具備している。その共通鍵３０は、認証手段２９を介して、デジタルインターフェースＤ－Ｉ／Ｆ３２に接続している。また、暗号化手段３１は、共通鍵３０を参照することが出来、デジタルインターフェース３２に接続している。デジタルＡＶデータ受信ユニットＴＶ３３も、共通鍵３６、認証手段３５、デジタルインターフェース３４、復号化手段３７を具備している。その共通鍵３６は認証手段３５を介してデジタルインターフェース３４に接続している。また、復号化手段３７は共通鍵３６を参照することが出来、デジタルインターフェース３４に接続している。さらにデジタルインターフェース３２とデジタルインターフェース３４は互いにデータのやり取りが出来る構成となっている。

【０００７】次にデジタルＡＶデータ送信ユニットＳＴＢ２８とデジタルＡＶデータ受信ユニットＴＶ３３間の動作を説明する。まず、デジタルＡＶ受信ユニットＴＶ３３が認証要求を出す。するとデジタルインターフェースＤ－Ｉ／Ｆ３４を通してデジタルＡＶ送信ユニットＳＴＢ２８を構成するデジタルインターフェースＤ－Ｉ／Ｆ３２に認証要求が到達する。デジタルインターフェースＤ－Ｉ／Ｆ３２は認証要求を受けて認証手段２９にて、共通鍵３０を参照して認証する。デジタルＡＶ送信ユニットＳＴＢ２８にて認証されれば、暗号化手段３１において、データが暗号化されて、デジタルインターフェースＤ－Ｉ／Ｆ３２を介して、暗号化したデータが送信される。これはデジタルインターフェースＤ－Ｉ／Ｆ３４を介して、共通鍵３６を参照してデジタ復号化手段３７で復号される。

【０００８】このようにすると、短い時間でデータの認証を行うことができる。しかし、共通鍵を用いた認証は偽造や改竄に弱いので、新作の映画など著作権上重要なデータの場合、第三者にデータを無料で視聴されることがある。またＴＶのように受信した全てのデータを表示するために、厳密な認証を行う機器と接続した場合に対応できる必要があり、デジタルＡＶデータ受信ユニットが厳密な認証を要する場合があり、そのような場合重要なデータの著作権が保護されないといったことが起こりうる。

【０００９】

【発明が解決しようとする課題】このように、あまり重要でないデータの認証に多くの時間を要するという課題や、重要なデータであるにもかかわらずその認証が偽造や改竄に弱いという課題が存在する。また、デジタルＡＶデータ受信ユニットによっては、厳密な認証を要しないものも存在し、このようなユニットに対して厳密な認証を行った場合、時間の無駄が生じるという課題や、逆にデジタルＡＶデータ受信ユニットによっては厳密な認証を要するものも存在し、そのようなユニットに厳密でない認証を行った場合、著作権が守られないといった課題が存在する。更に、不正使用の防止のために、厳密な認証と厳密でない認証とで、暗号鍵を各々に対応して用意した場合、厳密な認証を行って暗号鍵を取得した後に、厳密でないデータを必要とする場合でも、改めて厳密でない認証を行う必要がある。また、受信側が機器の排除機能を持たない機器の場合は、送信側は不正な機器を排除できない構成になっているという課題がある。

【００１０】本発明は、このような従来の、重要でないデータの認証に多くの時間を要するという課題と、重要なデータであるにもかかわらずその認証が偽造や改竄に弱いという課題と、ユニットによって認証に必要な厳密さが異なるといった課題を考慮し、データの重要性や相手の装置が有する認証方法の種別などを考慮して、適切な認証方法でデータの送受信を行いうるユニット、シ

ステム等を提供することを目的とするものである。

【００１１】

【課題を解決するための手段】上述した課題を解決するために、請求項１の本発明は、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、データ重要性判定手段の判定結果に基き、送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶデータ送信ユニットである。

【００１２】また請求項２の本発明は、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、データ重要性判定手段の判定結果に基き、送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶデータ送信ユニットを通信の対象とし、認証の要求を行う認証要求手段と、送信側複数認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたデジタルＡＶデータ受信ユニットである。

【００１３】また請求項３の本発明は、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、データ重要性判定手段の判定結果に基き、送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、認証の要求を行う認証要求手段と、送信側複数認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルＡＶデータ受信ユニットとを備えたデジタルＡＶデータ送受信システムである。

【００１４】また請求項４の本発明は、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、所定の管理基準を格納した管理基準格納手段と、認証要求を受け、データ重要性判定手段の判定結果に基き、管理基準格納手段の管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたデジタルＡＶデータ送信ユニットである。

【００１５】また請求項５の本発明は、送信ユニットは受信ユニットの各機能を有し、受信ユニットは送信ユニットの各機能を有する請求項３記載のデジタルＡＶデータ送受信システムである。

【００１６】また請求項６の本発明は、受信ユニットの機能を有する送信ユニット、あるいは送信ユニットの機能を有する受信ユニットが三つ以上互いに接続され、デジタルＡＶデータを互いにやりとりできる請求項５記載のデジタルＡＶデータ送受信システムである。

【００１７】また請求項７の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、デジタルＡＶデータ受信ユニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶ送信ユニットである。また請求項８の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、デジタルＡＶデータ受信ユニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットを通信の対象とし、認証の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側認証ルール格納手段と、認証ルールについての情報を送信する認証ルール情報送信手段と、送信ユニットとの間で認証ルールにて認証を行う受信側認証手段とを少なくとも備えたデジタルＡＶデータ受信ユニットである。

【００１８】また請求項９の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、デジタルＡＶデータ受信ユニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、認証

の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側認証ルール格納手段と、認証ルールについての情報を送信する認証ルール情報送信手段と、送信ユニットとの間で認証ルールにて認証を行う受信側認証手段を少なくとも有するデジタルＡＶデータ受信ユニットとを備えたデジタルＡＶデータ送受信システムである。

【００１９】また請求項１０の本発明は、所定の管理基準を格納した管理基準格納手段と、デジタルＡＶデータ受信ユニットから認証要求を受けて、そのデジタルＡＶデータ受信ユニットの種類又は重要度に応じて、管理基準格納手段の管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたデジタルＡＶ送信ユニットである。

【００２０】また請求項１１の本発明は、管理基準は、不正な、あるいは正当なデジタルＡＶデータ受信ユニットを識別できる基準リスト（ＣＲＬ）である請求項４又は１０に記載のデジタルＡＶ送信ユニットである。

【００２１】また請求項１２の本発明は、送信ユニットに、受信ユニットが二つ以上接続され、送信ユニットとの間で、デジタルＡＶデータをやりとりできる請求項９記載のデジタルＡＶデータ送受信システムである。

【００２２】また請求項１３の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、データ重要性判定手段の判定結果に基づき、送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、単一認証デジタルＡＶデータ受信ユニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、送信側認証選択手段又は送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶデータ送信ユニットである。

【００２３】また請求項１４の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、データ重要性判定手段の判定結果に基づき、送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、単一認証デジタルＡＶデータ受信ユニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、送信側認証選択手段又は送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも有するデジタルＡＶデータ送信ユニットと、認証の要求を行う認証要求手段と、送信側認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有する複数認証デジタルＡＶデータ受信ユニットと、認証の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側単一認証ルール格納手段と、認証ルールについての情報を送信する認証ルール情報送信手段と、デジタルＡＶデータ送信ユニットとの間で認証ルールにて認証を行う受信側認証手段を少なくとも有する単一認証デジタルＡＶデータ受信ユニットとを備えたデジタルＡＶデータ送受信システムである。

【００２４】また請求項１５の本発明は、複数認証デジタルＡＶデータ受信ユニットはデジタルＡＶデータ送信ユニットの各機能を有し、デジタルＡＶデータ送信ユニットは複数認証デジタルＡＶデータ受信ユニットの各機能を有する請求項１４記載のデジタルＡＶデータ送受信システムである。

【００２５】また請求項１６の本発明は、複数認証デジタルＡＶデータ受信ユニットの各機能を有するデジタルＡＶデータ送信ユニット、あるいはデジタルＡＶデータ送信ユニットの機能を有する複数認証デジタルＡＶデータ受信ユニットが二つ以上互いに接続され、且つ、単一認証デジタルＡＶデータ受信ユニットが二つ以上接続され、デジタルＡＶデータを互いにやりとりできる請求項１５記載のデジタルＡＶデータ送受信システムである。

【００２６】請求項１７の本発明は、デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証レベルの認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、認証の後、受信ユニットからの、暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、判定済みの認証レベルと同等及びそれ以下のレベルの解読情報の全部、又は一部を、受信ユニットに送信する解読情報選択手段とを備えた送信ユニットである。

【００２７】請求項１８の本発明は、データの重要度に応じた複数のレベルで暗号化されたデジタルＡＶデータを送信する送信ユニットから受信した暗号化されたデー

タを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を送信ユニットに要求する認証手段と、送信ユニットによる認証の後、認証レベルと同等及びそれ以下のレベルの暗号化データに対する解読情報の全部、又は一部を、送信ユニットに要求する解読情報要求手段とを備えた受信ユニットである。

【００２８】請求項１９の本発明は、デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証レベルの認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、認証の後、受信ユニットからの、暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、判定済みの認証レベルと同等及びそれ以下のレベルの解読情報の全部、又は一部を、受信ユニットに送信する解読情報選択手段とを有する送信ユニットと、その送信ユニットから受信した暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を送信ユニットに要求する認証手段と、送信ユニットによる認証の後、認証レベルと同等及びそれ以下のレベルの解読情報の全部、又は一部を、送信ユニットに要求する解読情報要求手段とを有する受信ユニットとを備えたデジタルＡＶデータ送受信システムである。

【００２９】請求項２０の本発明は、デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証レベルの認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、認証の後、受信ユニットからの、暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、判定済みの認証レベルと同等のレベルの解読情報を受信ユニットに送信する解読情報選択手段とを備え、解読情報選択手段は、次に受信ユニットから解読情報の要求があった時に、その要求が判定済みの認証レベルと同等あるいはそれ以下のレベルの解読情報の場合は、認証手続きを省略して要求された解読情報を受信ユニットに送信する送信ユニットである。

【００３０】請求項２１の本発明は、データの重要度に応じた複数のレベルで暗号化されたデジタルＡＶデータを送信する送信ユニットから受信した暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を送信ユニットに要求する認証手段と、送信ユニットによる認証の後、認証レベルと同等のレベルの暗号化データに対する解読情報を送信ユニットに要求する解読情報要求手段とを備え、解読情報要求手段は、認証のレベルと同等あるいはそれ以下のレベルの解読情報を送信ユニットに要求する時は、認証要求を行わずに、解読情報の要求を行う受信ユニットである。

【００３１】請求項２２の本発明は、デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証レベルの認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、認証の後、受信ユニットからの、暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、判定済みの認証レベルと同等のレベルの解読情報を受信ユニットに送信する解読情報選択手段とを有し、解読情報選択手段は、次に受信ユニットから解読情報の要求があった時に、その要求が判定済みの認証レベルと同等あるいはそれ以下のレベルの解読情報の場合は、認証手続きを省略して要求された解読情報を受信ユニットに送信する送信ユニットと、その送信ユニットから受信した暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を送信ユニットに要求する認証手段と、送信ユニットによる認証の後、認証レベルと同等のレベルの解読情報を送信ユニットに要求する解読情報要求手段とを備え、解読情報要求手段は、認証のレベルと同等あるいはそれ以下のレベルの解読情報を送信ユニットに要求する時は、認証要求を行わずに、解読情報の要求を行うとを有する受信ユニットとを備えたデジタルＡＶデータ送受信システムである。

【００３２】請求項２５の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、その送信側複数認証ルール格納手段から１種類の認証ルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶデータ送信ユニットであって、認証の要求を行い、送信側複数認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認証ルール格納手段から１種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルＡＶデータ受信ユニットまたは、送信ユニットにおける認証ルールの選択は、データの重要度の判定結果に基づいて行われ、重要度の判定を行ったユニットが重要度の判定を行わないユニットに選択した認証ルールについての情報を送り、重要度の判定を行わないユニットは、その情報に基づいて、同じ認証ルールを選択するデジタルＡＶデータ送信ユニットである。

【００３３】請求項２８の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証の要求を行い、デジタルＡＶデータの重要度を判定してその判定結果に基づいて、送信側複数認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認

証ルール格納手段から一種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルＡＶデータ受信ユニットで選択される認証ルールと同じルールを、送信側複数認証ルール格納手段から選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶデータ送信ユニットである。

【００３４】請求項３１の本発明は、複数種類の認証ルールから１種類の認証ルールを選択して認証を行う認証手段と、受信ユニットに対する所定の管理基準を格納した管理基準格納手段と、受信ユニットからの認証要求を受け、格納されている管理基準を参照することにより認証するか否かを判定する認証判定手段とを備えたデジタルＡＶデータ送信ユニットであって、認証要求を行う受信ユニットが、管理基準を持てない重要度の低い認証ルールのみで認証する機能しか有しない場合に、受信ユニットは、外部の管理センターからその受信ユニットに対応する管理基準用の識別情報が付与されるものであり、送信ユニットの認証判定手段は、認証要求の際に識別情報を受け取り、その識別情報が不可となった場合に、認証を取りやめるデジタルＡＶデータ送信ユニットである。

【００３５】請求項４３の本発明は、請求項１～４２のいずれかに記載のユニット又はシステムもしくは送信方法が有する各構成要素もしくはステップが持つ機能の全部又は一部を実現するためのプログラムを格納した媒体である。

【００３６】

【発明の実施の形態】以下に本発明の実施の形態を図面を参照して説明する。

【００３７】まず、第一の実施の形態について図１を参照して説明する。

【００３８】デジタルＡＶデータ送信ユニットＳＴＢ１は、データ重要性判定手段３、暗号化手段４、送信側複数認証ルール格納手段５、送信側認証選択手段６、送信側認証手段７及びデジタルインターフェースＤ－Ｉ／Ｆ８を持つ。このデータ重要性判定手段３は、データ２の重要性を重要度に応じて複数種類に場合分けを行う手段である。このデータの重要度はＣＧＭＳで表現されている。このＣＧＭＳは放送局から送られてくるデータの内部あるいはヘッダーに存在している。暗号化手段４は、データ２を、認証の過程で作成されたワーク鍵Ｋｃｏ１６で暗号化する手段である。ワーク鍵Ｋｃｏ１６を生成するその認証方法は後述する。送信側複数認証ルール格納手段５は、複数種類の認証ルールを持つ手段である。例えば、公開鍵と秘密鍵を用いた認証ルールと、共通鍵を用いた認証ルールの２種類の認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。送信側認証選択手段６は、送信側複数認証ルール格納手段５が持つ複数種類の認証ルールから一種類の認証ルールを選択する手段である。この際、データ重要性判定手段３の判定の結果を参考にする。本実施の形態では、前記の重要度が高いか低いかにより、時間はかかるが偽造や改竄に強い認証ルールとして、公開鍵と秘密鍵を用いた認証ルールを選択し、時間はかからないが、偽造や改竄に弱いルールとして、共通鍵を用いた認証ルールを選択する。送信側認証手段７は、選択された認証ルールで実際にデジタルＡＶデータ受信ユニットＴＶ９と認証をかわす手段である。デジタルインターフェースＤ－Ｉ／Ｆ８は、デジタルＡＶデータ受信ユニットＴＶ９とＡＶデータや信号のやりとりを行う手段である。

【００３９】デジタルＡＶデータ受信ユニットＴＶ９は、デジタルインターフェースＤ－Ｉ／Ｆ１０、復号化手段１１、認証要求手段１２、受信側認証手段１３、受信側複数認証ルール格納手段１４、受信側認証選択手段１５を持つ。この認証要求手段１２は、デジタルＡＶデータ送信ユニットＳＴＢ１に認証要求を出す手段である。また、受信側複数認証ルール格納手段１４は、送信側複数認証ルール格納手段５に格納された複数の認証ルールと同じ複数の種類の認証ルールを持つ手段である。従って本実施の形態の場合、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールを持つ。受信側認証選択手段１５は上述した受信側複数認証ルール格納手段１４から、送信側認証選択手段６で選択された認証ルールと同じ認証ルールを選択する手段である。受信側認証手段１３は、その選択された認証ルールで、つまりデジタルＡＶデータ送信ユニットＳＴＢ１で選択された認証ルールを用いて実際にデジタルＡＶデータ送信ユニットＳＴＢ１と認証を互いに交わす手段である。復号化手段１１はデジタルＡＶデータ送信ユニットＳＴＢ１で暗号化され送信されてきたデジタルＡＶデータをワーク鍵Ｋｃｏ１７を用いて復号化する手段である。ワーク鍵Ｋｃｏ１７は前記受信側認証過程で生成されるもので、その生成する方法は前記ワーク鍵Ｋｃｏ１６を生成する方法とともに後述する。デジタルインターフェースＤ－Ｉ／Ｆ１０は、送信ユニットＳＴＢ１とＡＶデータや信号のやりとりを行う手段である。

【００４０】次に、このような本実施の形態の動作を説明する。

【００４１】まず、デジタルＡＶデータ受信ユニットＴＶ９を構成する、認証要求手段１２が、デジタルインターフェースＤ－Ｉ／Ｆ１０を介して、デジタルＡＶデータ送信ユニットＳＴＢ１に自らのＩＤを含めて認証要求を出す。もちろんＡＶデータの送信要求も出す。デジタルＡＶデータ送信ユニットＳＴＢ１は、デジタルインターフェースＤ－Ｉ／Ｆ８を介して、前記認証要求を受信する。そうするとデジタルＡＶデータ送信ユニットＳＴＢ１は、まずデータ重要性判定手段３で、これから送信すべきＡＶデータ２の重要性を判定し場合分けする。す

なわちＣＧＭＳの値が１１なら重要度は高く、そのデータは表示のみ可能であり、コピーすることは禁止される。また、ＣＧＭＳの値が１０の場合は一回のみコピー可能であり、比較的重要なデータである。またＣＧＭＳが００の場合は自由に視聴ないしはコピーして使用してよいので、重要でないデータと言える。またＣＧＭＳが０１となるＡＶデータは存在しない。このＣＧＭＳの値によりデータの重要度の場合分けがなされる。この結果は送信側認証選択手段６に送られ、送信側複数認証ルール格納手段５から最適な認証ルールが選択される。すなわち、最新の映画など重要なデータの場合には、時間がかかるが、偽造や改竄に強い、公開鍵と秘密鍵を用いる認証ルールが選択される。また、ニュースのような重要でないデータの場合には、時間はかからないが、偽造や改竄に弱い、共通鍵を用いる認証ルールが選択される。更にその選択情報は、送信側認証手段７に送られ、デジタルインターフェースＤ－Ｉ／Ｆ８を介して、デジタルＡＶ受信ユニットＴＶ９に送られる。デジタルＡＶ受信ユニットＴＶ９においては、受信側認証選択手段１５が、その選択情報を利用して受信側複数認証ルール格納手段１４から、デジタルＡＶデータ送信ユニットＳＴＢ１で選択された認証ルールと同じ認証ルールを選択する。従って選択されている認証ルールは送信側と受信側とで同じになる。そこで、受信側認証手段１３と送信側認証手段７とは互いに、デジタルインタフェースＤ－Ｉ／Ｆ１０およびデジタルインタフェースＤ－Ｉ／Ｆ８を介して、認証を行う。認証が成功すれば、後述するようにして送信側にワーク鍵Ｋｃｏ１６、また受信側にワーク鍵Ｋｃｏ１７が生成される。送信すべきデータ２は生成されたワーク鍵Ｋｃｏ１６を用いて、暗号化手段４で暗号化される。そのあと、デジタルインターフェースＤ－Ｉ／Ｆ８を介して、デジタルＡＶデータ受信ユニットＴＶ９に暗号化データとして送信される。デジタルインターフェースＤ－Ｉ／Ｆ１０を介して暗号化されたデータは、ワーク鍵Ｋｃｏ１７を用いて、復号化手段１１にて復号化され、データ１０１になる。これはデータ２と同一のデータであり、デジタルＡＶデータ送信ユニットＳＴＢ１から、デジタルＡＶデータ受信ユニットＴＶ９にデータが送信されたことになる。

【００４２】最後に、デジタルＡＶデータ受信ユニットＴＶ９は、ディスプレイ装置の画面にそのデータを表示する。このようにして、データの重要性が高い時は、時間はかかるが、偽造や改竄に強い認証手段が用いられ、またデータの重要性が低い時は、時間はかからないが、偽造や改竄に弱い認証ルールが用いられる。

【００４３】次に前述したようにデジタルＡＶデータ受信ユニットＴＶ９からデジタル送信ユニットＳＴＢ１に認証要求が出たときの認証のやりとりを示し、その結果ワーク鍵Ｋｃｏを生成する実施の形態を図４と図５を参照して説明する。

【００４４】まず、図４に示すごとき、公開鍵と秘密鍵による認証を行う場合である。この場合受信側は秘密鍵Ｓｂと公開鍵Ｐｂを持つ。また送信側は秘密鍵Ｓａと公開鍵Ｐａを持つ。まずステップ１で受信側が乱数Ｂを発生する。受信側は自己の認識番号であるＩＤｂと乱数Ｂを自らの秘密鍵Ｓｂで暗号化した暗号文Ｓｂ（Ｂ）を送信側に送る。送信側は受信側の認識番号ＩＤｂから検索して受信側の公開鍵Ｐｂを入手する。ステップ８で入手した公開鍵Ｐｂで暗号文Ｓｂ（Ｂ）を復号化する。その結果ステップ９のごとく乱数Ｂが得られる。さらに、送信側は、ステップ１０のごとく乱数Ａを発生する。乱数ＡとＢは送信側の秘密鍵Ｓａで暗号化され暗号文Ｓａ（Ａ，Ｂ）が作成される。送信側は暗号文Ｓａ（Ａ，Ｂ）と自己の認識番号ＩＤａを受信側に送信する。受信側は暗号文Ｓａ（Ａ，Ｂ）と送信側の認識番号ＩＤａを受け取る。受信側は、送信側の認識番号ＩＤａから検索して送信側の公開鍵Ｐａを入手し、ステップ２のごとく、Ｐａで暗号文Ｓａ（Ａ，Ｂ）を復号化する。ここで、暗号文Ｓａ（Ａ，Ｂ）から受信側にはステップ１で送った乱数Ｂと全く同一の乱数Ｂが得られ、偽造や改竄が行われてないことが受信側にわかる。もし前記２つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。但し、この場合は、公開鍵Ｐａ，Ｐｂは正当な者にしか入手できないようになっているものとする。次に受信側はステップ３のごとく、受信側の秘密鍵Ｓｂで乱数Ａを暗号化し、暗号文Ｓｂ（Ａ）を作成する。Ｓｂ（Ａ）は送信側に送られ、ステップ１１のごとく既に送信側で持っている、受信側の公開鍵Ｐｂで暗号文Ｓｂ（Ａ）を復号化する。ステップ１０で発生した、乱数Ｂとステップ１１で復号化した乱数Ｂは全く同一であれば、偽造や改竄が行われていないことが送信側にわかる。もし前記２つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。

【００４５】今、受信側と送信側でやりとりした乱数ＡとＢは偽造や改竄が行われていないとすると、受信側と送信側以外の第３者には乱数ＡとＢは秘密の乱数である。そこで送信側で、ステップ１２のごとく、乱数ＡとＢを用いて鍵Ｋａｂを作成する。同じくステップ４のごとく受信側で乱数ＡとＢを用いて鍵Ｋａｂを作成する。前記２つのＫａｂは全く同一のものであり共通鍵となっている。次に送信側でステップ１３のごとく鍵Ｋｅｘを作成する。これを共通鍵Ｋａｂで暗号化し、暗号文Ｋａｂ（Ｋｅｘ）を作成して、受信側に送る。受信側はステップ５のごとく共通鍵Ｋａｂで暗号文Ｋａｂ（Ｋｅｘ）を復号化してＫｅｘを得、その結果、受信側が得た鍵Ｋｅｘと送信側にある鍵Ｋｅｘは全く同一であり、共通鍵となる。次に送信側でステップ１４のごとく鍵Ｋｃｏを作成する。鍵Ｋｃｏは共通鍵Ｋｅｘで暗号化され、暗号文Ｋｅｘ（Ｋｃｏ）として、受信側に送られる。受信側では、ステップ６のごと

く共通鍵Ｋexで暗号文Ｋex（Ｋco）を復号化し、ステップ７のごとくＫcoを得る。送信側にある鍵Ｋcoと受信側にあるＫcoは全く同一で、共通鍵となっている。以上が公開鍵と秘密鍵による認証の過程で得られたワーク鍵Ｋcoである。

【００４６】次に図５に示すごとき、共通鍵による認証を行う場合の説明をする。この場合、送信側と受信側は共通鍵Ｓを持つ。なお、この共通鍵は正当な者にしか与えられていない。まず,受信側でステップ１５のごとく２個の乱数Ａ１，Ａ２を発生し、共通鍵Ｓで暗号化し、暗号文Ｓ（Ａ１Ａ２）を作成し、送信側へ送る。送信側ではステップ２０のごとく共通鍵Ｓで暗号文Ｓ（Ａ１Ａ２）を復号化する。そうすると、ステップ２１のごとく乱数Ａ１と乱数Ａ２が得られる。送信側は乱数Ａ２を受信側に送る。受信側はステップ１６のごとく２つの乱数Ａ１とＡ２を持つことになる。ステップ１５で発生した乱数Ａ２とステップ１６で送信側から受け取った乱数Ａ２が全く同じであれば、送信側で偽造や改竄が行われていないことがわかる。もし、上記２つの乱数が異なっていれば偽造や改竄が行われたことになり認証は失敗する。次に送信側はステップ２２のごとく乱数Ｂ１とＢ２を発生し、暗号化して、暗号文Ｓ（Ｂ１Ｂ２）を受信側に送る。受信側はステップ１７のごとく共通鍵Ｓを用いて暗号文Ｓ（Ｂ１Ｂ２）を復号化する。すると、ステップ１８のごとく乱数Ｂ１とＢ２が得られる。受信側は乱数Ｂ２を送信側に送る。送信側はステップ２３のごとく乱数Ｂ１とＢ２を持つことになる。ステップ２２で発生した乱数と、ステップ２３で受信側から受け取った乱数Ｂ２が同じであれば、受信側に、偽造や改竄が行われていないことがわかり、認証は成功する。もし、上記２つの乱数が異なっていれば、偽造や改竄が行われたことになり認証は失敗である。

【００４７】ここまでで、認証が成功しているとすると、乱数Ａ１と乱数Ｂ１は送信側と受信側以外の第３者には秘密の乱数である。送信側ではステップ２４のごとく乱数Ａ１と乱数Ｂ1から鍵Ｋcoを作成する。一方受信側では、ステップ１９のごとく乱数Ａ１と乱数Ｂ１から鍵Ｋcoを作成する。送信側にある鍵Ｋcoと受信側にある鍵Ｋcoは全く同一であり、共通鍵となっている。以上が共通鍵による認証の過程で得られたワーク鍵Ｋcoである。

【００４８】なお、本発明において、選択する認証ルールの種類は、前記公開鍵及び秘密鍵と共通鍵との２種類に限らず、その他の種類でもよく、更に３種類以上の異なる認証ルールを使用するものであってもよい。

【００４９】また、本実施の形態の変形例として、デジタルＡＶデータ送信ユニット１はデジタルAV受信ユニット９と同じ機能を有し、また、デジタルＡＶデータ受信ユニット９はデジタルＡＶ送信ユニット１と同じ機能を有するようになっていてもよい。以後それらのユニットのことを、デジタルＡＶデータ送受信ユニットと呼ぶ。またそれらの送受信ユニットが３台以上が互いに接続されていてもよい。

【００５０】次に本発明の第二の実施の形態について図６を参照して説明する。

【００５１】本実施の形態では、第一の実施の形態がデータの重要度に応じて認証ルールを変えていたのに対して、デジタルＡＶデータ受信ユニットＶＴＲ４５が有する認証ルールの種類によって、認証ルールを選択するところが、相違点である。

【００５２】デジタルＡＶデータ送信ユニットＳＴＢ３８は、送信側複数認証ルール格納手段４１等を持つ。送信側複数認証ルール格納手段４１は、複数種類の認証ルールを持つ手段である。これは第一の実施の形態で説明したごとく、例えば、公開鍵と秘密鍵を用いた認証ルールと、共通鍵を用いた認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。ユニット認証ルール情報受信手段４２は、デジタルＡＶデータ受信ユニットＶＴＲ４５から送られて来た認証ルールに関連する情報を受信する手段である。送信側認証取り出し手段５３は、その認証ルールに関連する情報に基づいて、送信側複数認証ルール格納手段４１から所定の認証ルールを取り出し、送信側認証手段４３に渡す手段である。送信側認証手段４３は、デジタルＡＶ受信ユニットＶＴＲ４５と互いに認証を交わす手段である。暗号化手段４０は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵Ｋco５３により、データ３９を暗号化する手段である。デジタルインターフェースＤ－Ｕ／Ｆ４４は、デジタルＡＶデータ受信ユニットＶＴＲ４５とデータや信号のやりとりをする手段である。

【００５３】デジタルＡＶデータ受信ユニットＶＴＲ４５は、受信側認証ルール格納手段４９等を持つ。この受信側認証ルール格納手段４９は、第一の実施の形態で説明した場合とは違って、一種類の認証ルールのみ格納する手段である。例えば、公開鍵と秘密鍵を用いた認証ルール、あるいは共通鍵を用いた認証ルールのような認証ルールがある。ここで、受信側認証ルール格納手段４９に格納されている認証ルールはデジタルＡＶデータ受信ユニットＶＴＲ４５の装置の性質あるいは重要度によって、あらかじめ決められている。すなわちデータの再利用を予定しないＴＶなどのユニットには時間はかかるが、偽造や改竄に強い認証ルールが格納されており、またデータのコピーを前提とするＶＴＲのようなユニットには、時間はかからないが、偽造や改竄に弱い認証ルールが格納されている。これによって、ＡＶデータの著作権を守ることができる。本実施の形態では　デジタルＡＶデータ受信ユニットＶＴＲ４５はＶＴＲであるので、受信側認証ルール格納手段４９は共通鍵を持つものとし

て説明をする。認証ルール情報送信手段５０は、デジタルＡＶデータ受信ユニットＶＴＲ４５が受信側認証ルール格納手段４９に有する共通鍵による認証ルールに関連する情報を送信する手段である。受信側認証手段５１は、デジタルＡＶ送信ユニットＳＴＢ３８と互いに認証を交わす手段である。復号化手段４７は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵Ｋco５４により、暗号化されたデータを復号化する手段である。

【００５４】次にこのような本実施の形態の動作を説明する。

【００５５】まず、デジタルＡＶデータ受信ユニットＶＴＲ４５を構成する、認証要求手段４８がデジタルインターフェースＤ－Ｉ／Ｆ４６を介して、デジタルＡＶデータ送信ユニットＳＴＢ３８に認証要求を出す。デジタルＡＶデータ送信ユニットＳＴＢ３８は、デジタルインターフェースＤ－Ｉ／Ｆ４４を介して、前記認証要求を受信する。また同時に、認証ルール情報送信手段５０が、受信側認証ルール格納手段４９を参照し、格納されている認証ルール、つまり共通鍵による認証ルールに関する情報を取り出す。例えば、その共通鍵による認証ルールを示す識別子を、デジタルインターフェースＤ－Ｉ／Ｆ４６を介して、デジタルＡＶデータ送信ユニットＳＴＢ３８に送る。ユニット認証ルール情報受信手段４２が、デジタルＡＶデータ受信ユニットＶＴＲ４５から送られてきた認証ルールに関する情報、つまり共通鍵による認証ルールの識別子を、デジタルインターフェースＤ－Ｉ／Ｆ４４を介して、受け取る。さらに、この認証ルールの識別子は、送信側認証ルール取り出し手段５５に渡され、送信側複数認証ルール格納手段４１から、その認証ルールに関する情報に応じた認証ルール、つまり共通鍵による認証ルールを取り出す。その後、取り出された共通鍵による認証ルールは、送信側認証手段４３に渡される。その後、送信側認証手段４３と受信側認証手段５１は互いに、デジタルインターフェースＤ－Ｉ／Ｆ４４とＤ－Ｉ／Ｆ４６を介して、認証を交わす。認証が成功すれば、その結果、第一の実施の形態で説明したごとく、送信側にワーク鍵Ｋco５３、受信側にワーク鍵Ｋco５４が生成される。データ３９は暗号化手段４０にてワーク鍵Ｋco５３により暗号化される。暗号化されたデータはデジタルインターフェースＤ－Ｉ／Ｆ４４を介して、デジタルＡＶ受信ユニットＶＴＲ４５に送られる。デジタルインターフェースＤ－Ｉ／Ｆ４６を介して暗号化されたデータは、復号化手段４７に送られ、ワーク鍵Ｋco５４を用いて復号化され、データ５２が得られる。

【００５６】なお、本発明において、送信側の認証ルールの種類は、前記共通鍵に限らず、公開鍵及び秘密鍵、またその他の種類でもよく、更に３種類以上の異なる認証ルールを使用するものであってもよい。

【００５７】また、デジタルＡＶデータ受信ユニットは２台あり、その一つは共通鍵による認証ルールのみ有し、他の一つは公開鍵及び秘密鍵のみを有するものであってもよい。さらに３台以上のデジタルＡＶデータ受信ユニットであってもよい。

【００５８】次に本発明の第三の実施の形態について図７を参照して説明する。

【００５９】第一の実施の形態がデータの重要度に応じて認証ルールを変えていたのに対し、また、第二の実施の形態がデジタルＡＶデータ受信ユニットの種類によって認証ルールを変えていたのに対し、本実施の形態では、データの重要度とデジタルＡＶ受信ユニットの種類の両方で認証ルールを決めるところが特徴である。

【００６０】本実施の形態では、デジタルＡＶデータ送信ユニットＳＴＢ５６と、複数認証デジタルＡＶデータ受信ユニットＴＶ６５と、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２の三種類のユニットを扱う。デジタルＡＶデータ送信ユニットＳＴＢ５６は複数認証デジタルＡＶデータ受信ユニットＴＶ６５と単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２にデータを送信するユニットである。複数認証デジタルＡＶデータ受信ユニットＴＶ６５に対しては、デジタルＡＶデータ送信ユニットＳＴＢ５６においてデータの重要度により複数種類の認証ルールを選択して、そのデータを送信する。また、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２は自らの持つ一つの認証ルールを用いてデジタルＡＶデータ送信ユニット ＳＴＢ５６とで認証を行うユニットである。

【００６１】デジタルＡＶデータ送信ユニットＳＴＢ５６は、データ重要性判定手段５７を持つ。これは、データ８２の重要性を重要度に応じて複数種類の場合分けを行う手段である。この重要度は第一の実施の形態で説明したごとくＣＧＭＳで表現されている。このＣＧＭＳは放送局から送られてくるデータの内部あるいはヘッダーに存在している。暗号化手段６４は、データ８２を認証の過程で作成されたワーク鍵Ｋco７９で暗号化する手段である。ワーク鍵Ｋco７９を生成する過程は第一の実施の形態で説明した。送信側複数認証ルール格納手段６３は、複数種類の認証ルールを持つ。例えば、公開鍵と秘密鍵を用いた認証ルールや、共通鍵を用いた認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。送信側認証選択手段５９は、送信側複数認証ルール格納手段６３が持つ複数種類の認証ルールから一種類の認証ルールを選択する手段である。この時、データ重要性判定手段５７の場合分けの結果を参考にする。第一の実施の形態のごとく、本実施の形態では、前記の重要度が高いか低いかにより、時間はかかるが偽造や改竄に強い認証ルールとして、公開鍵と秘密鍵を用いた認証ルールを選択し、また、時間はかからないが、偽造や改竄に弱い認証ルールとして、共通鍵を用いた認証

ルールを選択する。ユニット認証ルール情報受信手段６０は、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２から送られて来た認証ルールに関する情報を受信する手段である。送信側認証ルール取り出し手段５８は、認証ルールに関連する情報に基づいて、送信側複数認証ルール格納手段６３から所定の認証ルールを取り出し、送信側認証手段６１に渡す手段である。送信側認証手段６１は、実際に複数認証デジタルＡＶデータ受信ユニットＴＶ６５及び単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２と認証を交わす手段である。デジタルインターフェースＤ－Ｉ／Ｆ６２は、複数認証デジタルＡＶデータ受信ユニットＴＶ６５や単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２とＡＶデータや信号をやりとりする手段である。

【００６２】複数認証デジタルＡＶデータ受信ユニットＴＶ６５は、認証要求手段６７を持つ。これは、デジタルＡＶデータ送信ユニットＳＴＢ５６に認証要求を出す手段である。また、受信側複数認証ルール格納手段６８は、送信側複数認証ルール格納手段６３と同じ複数種類の認証ルールを持つ。従って本実施の形態の場合、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールがある。受信側認証選択手段６９は、受信側複数認証ルール格納手段６８から、送信側認証選択手段５９で選択された認証ルールと同じ認証ルールを選択する手段である。受信側認証手段７０は、その選択された認証ルールで、つまりデジタルＡＶデータ送信ユニットＳＴＢ５６で選択された認証ルールを用いて実際にデジタルＡＶデータ送信ユニットＳＴＢ５６と認証を互いに交わす手段である。復号化手段６６は、デジタルＡＶデータ送信ユニットＳＴＢ５６で暗号化されたデジタルＡＶデータをワーク鍵Ｋco８０を用いて復号化する手段である。ワーク鍵Ｋco８０は前記認証過程で生成されるもので、その生成する方法は前記ワーク鍵Ｋco７９とともに第一の実施の形態で説明した。デジタルインターフェースＤ－Ｉ／Ｆ７１は、デジタルＡＶデータ送信ユニットＳＴＢ５６とＡＶデータや信号のやりとりを行う手段である。

【００６３】単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２は、受信側認証ルール格納手段７５を持つ。これは、前述したごとく一種類の認証ルールのみ格納する手段である。例えば、公開鍵と秘密鍵を用いた認証ルール、あるいは共通鍵を用いた認証ルールのような認証ルールがある。ここで、受信側認証ルール格納手段７５に格納されている認証ルールは単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２の装置の種類や、重要度によって、あらかじめ決められている。ここでは、受信側認証ルール格納手段７５が共通鍵を持つものとして説明をする。認証ルール情報送信手段７６は、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２が受信側認証ルール格納手段７５に有する共通鍵による認証ルールに関連する情報を送信する手段である。受信側認証手段７７は、デジタルＡＶデータ送信ユニットＳＴＢ５６と互いに認証を交わす手段である。復号化手段７３は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵Ｋco８１により、暗号化されたデータを復号化する手段である。

【００６４】次にこのような本実施の形態の動作を説明する。まず、はじめに複数認証デジタルＡＶデータ受信ユニットＴＶ６５かまたは単一認証デジタルＡＶデータ受信ユニット７２が認証要求を出す。デジタルＡＶデータ送信ユニットＳＴＢ５６はどのユニットから認証要求が送られて来たのかを判断する。

【００６５】以下、まず複数認証デジタルＡＶデータ受信ユニットＴＶ６５から認証要求が来た場合を説明し、次に単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２から認証要求が来た場合の説明を行う。

【００６６】第一に、前述したように複数認証デジタルＡＶデータ受信ユニットＴＶ６５を構成する、認証要求手段６７が、デジタルインターフェースＤ－Ｉ／Ｆ７１を介して、デジタルＡＶデータ送信ユニットＳＴＢ５６に自らのＩＤを含めて認証要求を出す。デジタルＡＶデータ送信ユニットＳＴＢ５６は、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、前記認証要求を受信する。そうするとデジタルＡＶデータ送信ユニットＳＴＢ５６は、まずデータ重要性判定手段５７で、これから送信すべきデータ８２の重要性を判定し場合分けする。この結果は送信側認証選択手段５９に送られ、送信側複数認証ルール格納手段６３から最適な認証ルールが選択される。すなわち、重要なデータの場合には、公開鍵と秘密鍵を用いる認証ルールが選択される。また、重要でないデータの場合には、共通鍵を用いる認証ルールが選択される。更にその選択情報は、送信側認証手段６１に送られ、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、複数認証デジタルＡＶデータ受信ユニットＴＶ６５に送られる。複数認証デジタルＡＶデータ受信ユニットＴＶ６５においては、受信側認証選択手段６９が、その選択情報を利用して受信側複数認証ルール格納手段６８からデジタルＡＶデータ送信ユニットＳＴＢ５６で選択された認証ルールと同じ認証ルールを選択する。従って選択されている認証ルールは送信側と受信側とで同じになる。受信側認証手段７０と送信側認証手段６１とは互いに、デジタルインターフェースＤ－Ｉ／Ｆ７１およびデジタルインターフェースＤ－Ｉ／Ｆ６２を介して、認証を行う。認証が成功すれば、第一の実施の形態で詳述したごとく、送信側にワーク鍵Ｋco７９、また受信側にワーク鍵Ｋco８０が生成される。送信すべきデータ８２は生成されたワーク鍵Ｋco７９を用いて、暗号化手段６４で暗号化される。そのあと、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、複数認証デジタルＡＶデータ受信ユニットＴＶ６５に暗号化されたデータとして送

信される。デジタルインターフェースＤ－Ｉ／Ｆ７１を介して暗号化されたデータは、ワーク鍵Ｋco８０を用いて、復号化手段６６にて復号化され、データ８３になる。これはデータ８２と同一のデータであり、デジタルＡＶデータ送信ユニットＳＴＢ５６から、複数認証デジタルＡＶデータ受信ユニットＴＶ６５にデータが送信されたことになる。このようにして、データの重要性が高い時は、時間はかかるが、偽造や改竄に強い認証ルールが用いられ、またデータの重要性が低い時は、時間はかからないが、偽造や改竄に弱い認証ルールが用いられる。

【００６７】次に単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２から認証要求が来た場合の動作の説明を行う。まず、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２を構成する、認証要求手段７４がデジタルインターフェースＤ－Ｉ／Ｆ７８を介して、デジタルＡＶデータ送信ユニットＳＴＢ５６に認証要求を出す。デジタルＡＶデータ送信ユニットＳＴＢ５６は、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、前記認証要求を受信する。同時に認証ルール情報送信手段７６が、受信側認証ルール格納手段７５を参照し、格納されている認証ルール、つまり共通鍵による認証ルールに関する情報を取り出す。例えば、その共通鍵による認証ルールを示す識別子を、デジタルインターフェースＤ－Ｉ／Ｆ７８を介して、デジタルＡＶデータ送信ユニットＳＴＢ５６に送る。ユニット認証ルール情報受信手段６０が、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２から送られてきた認証ルールに関する情報、つまり共通鍵による認証ルールの識別子を、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、受け取り、さらにこの認証ルールの識別子は、送信側認証ルール取り出し手段５８に渡される。送信側認証ルール取り出し手段５８は、送信側複数認証ルール格納手段６３から、その認証ルールに関する情報に応じた認証ルール、つまり共通鍵による認証ルールを取り出し、送信側認証手段６１に渡す。送信側認証手段６１と受信側認証手段７７は互いに、デジタルインターフェースＤ－Ｉ／Ｆ６２とＤ－Ｉ／Ｆ７８を介して、認証を交わす。認証が成功すれば、その結果、第一の実施の形態で詳述したごとく、送信側にワーク鍵Ｋco７９、受信側にワーク鍵Ｋco８１が生成される。認証の結果ワーク鍵が生成される過程は、第一の実施の形態で詳述した。

【００６８】データ８２は暗号化手段６４にてワーク鍵Ｋco７９により暗号化される。暗号化されたデータはデジタルインターフェースＤ－Ｉ／Ｆ６２を介して、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２に送られる。デジタルインターフェースＤ－Ｉ／Ｆ７８を介して受信した暗号化されたデータは、復号化手段７３に送られ、ワーク鍵Ｋco８１を用いて復号化され、データ８４が得られる。これはデータ８２と同一のデータであり、デジタルＡＶデータ送信ユニットＳＴＢ５６から、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２にデータが送信されたことになる。

【００６９】次に、本発明の第四の実施の形態を説明する。

【００７０】本実施の形態では、デジタルＡＶデータ受信ユニットが正当なものか不正なものかを調べて作成しておいた管理基準（ＣＲＬ）を利用するものである。そのＣＲＬの作成の仕方は、例えば、消費者が購入した販売店が発行した登録カードを元に作成する方法等が考えれれる。

【００７１】図８は、その管理基準を放送局から送られてくるデジタルＡＶデータの重要度に応じて、その管理基準を参照するかどうか決定するものである。

【００７２】デジタルＡＶ送信ユニットＳＴＢ９３は、放送局から送られてくるデジタルＡＶデータの重要度に応じて、データの重要性を判定する、データ重要性判定手段８６を有する。また、データの重要度に応じて管理基準格納手段８８に格納されている管理基準情報（ＣＲＬ）を参照するかどうかを判定する、管理基準参照決定手段８７を有する。また、前記決定結果に従って、認証を行うかどうかを決定する、認証決定手段８９を有する。また、実際にデジタルＡＶデータ受信ユニットＴＶ９２と認証を交わす、認証手段９０を有する。前記認証手段９０は、デジタルインターフェースＤ－Ｉ／Ｆ９１を介して、デジタルＡＶデータ受信ユニットＴＶ９２に接続している。

【００７３】次に本実施の形態の動作を説明する。まず、放送局から送られてくるデジタルＡＶデータ８５は、データ重要性判定手段８６で、重要性を判定される。その結果は、管理基準参照決定手段８７に渡され、管理基準格納手段８８に格納されている情報を参照すべきかどうかが決定される。例えば、新作の映画等の場合は重要なので、管理基準情報を参照すると決定する。また、ニュース等の場合は重要でないので、管理基準情報を参照しないと決定する。さらに認証決定手段８９で、前記管理基準参照決定手段８７の判定決定に従って、認証すべきかどうか決定される。すなわち、デジタルＡＶデータ受信ユニットＴＶ９２が、デジタルＡＶデータ８５を受信するのに正当な機器か不当な機器かを、管理基準格納手段８８に格納されている管理基準情報で判断される。正当であると判断されれば、次の認証手段９０で、デジタルインターフェースＤ－Ｉ／Ｆ９１を介して、デジタルＡＶ受信ユニットＴＶ９２と認証が交わされる。不当と判断されればその時点で、デジタルＡＶデータ受信ユニットＴＶ９２との認証は交わされず、データ８５の送信はされない。

【００７４】他方、図９は上述した管理基準を、デジタルＡＶデータ受信ユニットの装置の種類、あるいは重要度に応じて、その管理基準を参照するかどうか決定する

ものである。

【００７５】デジタルＡＶデータ送信ユニットＳＴＢ９４は、デジタルＡＶデータ受信ユニットＶＴＲ１００の装置の種類あるいは、重要度に応じて、その管理基準格納手段９６を参照すべきかどうかを決定する、管理基準参照決定手段９５を有する。また、認証決定手段９７は、認証するかどうかを決定する。管理基準格納手段９６は、デジタルＡＶデータ受信ユニットＶＴＲ１００がデジタルＡＶデータを受信するのに正当な機器か正当でない機器かの情報が格納されている。認証手段９８は、デジタルインターフェースＤ－Ｉ／Ｆ９９を介して、デジタルＡＶデータ受信ユニットＶＴＲ１００と認証を行う。

【００７６】次に本実施の形態の動作を説明する。まず、デジタルＡＶデータ受信ユニットＶＴＲ１００が、デジタルインターフェースＤ－Ｉ／Ｆ９９を介して、管理基準参照決定手段９５に機器情報を送る。これを受けて、管理基準参照決定手段９５は、管理基準格納手段９６に格納されている情報を参照すべきかどうかを決定する。管理基準格納手段９６を参照すると決定された場合は、認証決定手段９７は、まず、管理基準格納手段９６を参照して、デジタルＡＶデータ受信ユニットがデータを受信するのに正当な機器か、不正な機器かを判定する。ここで、正当な機器と判定されれば、次の認証手段９８にて、デジタルインターフェースＤ－Ｉ／Ｆ９９を介して、デジタルＡＶデータ受信ユニットと認証を開始する。デジタルＡＶデータ受信ユニットがデータを受信するのに不正な機器と判定された場合は、認証は行われず、データの送信も行われない。

【００７７】なお、上記実施の形態では、ＳＴＢを送信ユニットとして説明してきたが、ＶＴＲで録画したデータを再生する際には、ＶＴＲが送信ユニットとなる。この際ＣＧＭＳが入力時「１回コピー可」であれば「コピー不可」に書きかえられて出力される。ここで、データの重要度としては、元の入力時における重要度と考えるべきであり、「１回コピー可」と同様の認証ルールを使うこともできる。このように「１回コピーの結果コピー不可となったデータ」と「元からコピー不可のデータ」を見分ける必要がある際には、前述した、存在しないＣＧＭＳ値０１を前者の区別用に割り当てることもできる。

【００７８】次に本発明の第五の実施の形態について説明する。

【００７９】図１０は、本発明の第五の実施の形態についての概略図である。本実施の形態では、認証手続きのレベル２段階、コンテンツの重要度、すなわち、解読情報としての暗号鍵を３種類としている。図１０において、デジタルＡＶデータ送受信システムは、送信ユニット１１１と、それに接続された受信ユニット１３０により構成されている。

【００８０】送信ユニット１１１は、コンテンツ重要度が異なるデータＡ，Ｂを各々異なる暗号鍵Ｋcoで暗号化する暗号化手段Ａ，Ｂ１１２，１１３と、暗号化用の例えば、ｃｏｐｙ＿ｎｅｖｅｒ（テープ等に記録してはいけないコンテンツ）用Ｋco、ｃｏｐｙ＿ｏｎｃｅ（一度だけ記録してもよいコンテンツ）用Ｋco、ｎｏ＿ｍｏｒｅ＿ｃｏｐｙ（これ以上コピーしてはならないコンテンツ）用Ｋcoを記憶するＫco記憶手段１１４と、受信ユニット１３０に渡す、′Ｅｘｃｈａｎｇｅ＿Ｋｅｙ′と呼ばれるｃｏｐｙ＿ｎｅｖｅｒ用、ｃｏｐｙ＿ｏｎｃｅ用、ｎｏ＿ｍｏｒｅ＿ｃｏｐｙ用の各暗号鍵Ｋexを発生するＫex発生手段１１５と、その発生した各Ｋexを記憶するＫex記憶手段１１６と、暗号化用鍵Ｋcoを所定の関数により算出する時に用いる種を発生する種発生手段１１７と、その発生した種を記憶する種記憶手段１１８と、Ｋex記憶手段１１６からのＫexと種記憶手段１１８からの種を用いて、関数Ｋco＝ｆ（種、Ｋex）によりＫcoを算出するＫco算出手段１１９と、受信ユニット１３０に対して認証手続きを実行する認証手段１２１と、受信ユニット１３０の認証済みのレベルを判定する等の処理を行うレベル判定手段１２２と、受信ユニット１３０からの種要求に対して応答する種要求コマンド応答手段１２０と、データの送受信を行うデジタルインターフェース（Ｄ－Ｉ／Ｆ）１２３により構成されている。ここで、種要求コマンド応答手段１２０及び認証手段１２１の一部などが解読情報選択手段を構成している。

【００８１】また、受信ユニット１３０は、データの送受信を行うデジタルインターフェース（Ｄ－Ｉ／Ｆ）１３１と、受信した暗号化デジタルＡＶデータのコンテンツの重要度に応じて、要求する認証のレベルを決定する要求レベル決定手段１３４と、その決定された要求レベルで、送信ユニット１１１に認証を要求し、必要な暗号鍵Ｋexを取得する認証手段１３３と、その取得したＫexを記憶するＫex記憶手段１３７と、種の要求コマンドを発行し、種を送信ユニット１１１から取得する種要求コマンド発行手段１３５と、その取得した種とＫex記憶手段１３７に記憶されたＫexとを用いて、送信ユニット１１１と同一の関数Ｋco＝ｆ（種、Ｋex）によりＫcoを算出するＫco算出手段１３６と、その算出したＫcoにより暗号化データを復号する復号化手段１３２により構成されている。ここで、種要求コマンド発行手段１３５及び認証手段１３３の一部などが解読情報要求手段を構成している。

【００８２】次に、上記実施の形態のデジタルＡＶデータ送受信システムの動作について、図面を参照しながら説明する。

【００８３】図１１において、まず、受信ユニット１３０では、要求レベル決定手段１３４が受信データのコンテンツ重要度に基づいて要求する認証のレベルを決定し、認証手段１３３に渡す。認証手段１３３はＤ－Ｉ／

Ｆ１３１を介して送信ユニットに認証要求を出す。ここでは、一番高いレベルの認証を要求するものとする。送信ユニット１１１では、Ｄ－Ｉ／Ｆ１２３を介して受け取った認証要求に基づいて認証処理を行う。認証の方法については、例えば前述した実施の形態で説明した方法等により行うことができ、このとき送信ユニット、受信ユニットともに共有の共通鍵Ｋabが得られる。又、このときの認証済みのレベルがレベル判定手段１２２に渡される。

【００８４】次に、認証が完了してその通知が受信ユニット１３０に送信されると、認証手段１３３は、認証レベルが最高であることから、送信ユニット１１１に対して全てのレベルのＫexを要求する。ここでは、Ｋexのレベルとして、高い順にｃｏｐｙ＿ｎｅｖｅｒ用（Ｋex1）、ｃｏｐｙ＿ｏｎｃｅ用（Ｋex2）、ｎｏ＿ｍｏｒｅ＿ｃｏｐｙ用（Ｋex3）の３種類とする。

【００８５】送信ユニット１１１では、レベル判定手段１２２が、認証手段１２１から受けた要求レベルを認証済みレベルに基づいて判定し、渡せるか否かの判定と、渡せる場合は、要求のあったＫex（このときは、Ｋex1、Ｋex2、Ｋex3）を両者が共有するＫabで暗号化して、認証手段１２１を通じて受信ユニット１３０に送信する。受信ユニット１３０では、認証手段１３３が暗号化されたＫab（Ｋex1、Ｋex2、Ｋex3）を自身の持つＫabで復号してＫex記憶手段１３７に記憶する。

【００８６】一方、Ｋex発生手段１１５が発生した各レベルのＫex、すなわち、Ｋex1、Ｋex2、Ｋex3は、Ｋex記憶手段１１６に記憶され、種発生手段１１７が発生した種は、種記憶手段１１８に記憶されている。又、Ｋex記憶手段１１６に記憶された各Ｋexと、種記憶手段１１８に記憶された種とを用いて、Ｋco算出手段１１９が各Ｋco、すなわち、ｃｏｐｙ＿ｎｅｖｅｒ用（Ｋco1）、ｃｏｐｙ＿ｏｎｃｅ用（Ｋco2）、ｎｏ＿ｍｏｒｅ＿ｃｏｐｙ用（Ｋco3）を算出してＫco記憶手段１１４に記憶している。更に、暗号化手段Ａ，Ｂ１１２，１１３は、各データのコンテンツの重要度に対応したＫcoを用いてデジタルＡＶデータを暗号化して受信ユニット１３０に送信する。

【００８７】受信ユニット１３０では、種要求コマンド発行手段１３５が種要求コマンドを送信ユニット１１１に送信する。そうすると、送信ユニット１１１では、種要求コマンド応答手段１２０が、種記憶手段１１８から種を取り出し受信ユニット１３０に送信する。ここで、図の種記憶手段１１８に現在の種及び次の種とあるのは、暗号化用のＫcoを刻々と変更しているためである。

【００８８】次に、受信ユニット１３０では、種要求コマンド発行手段１３５が送信ユニット１１１から受け取った種と、Ｋex記憶手段に記憶している復号化するデータのレベルに対応するＫexとを用いて、Ｋco算出手段１３６は、送信ユニット１１１と同一の関数（この関数は、送信ユニット及び受信ユニットが予め持っており、第３者は入手できないものとする）によりＫcoを算出する。復号化手段１３２はこの算出されたＫcoを用いて暗号化されたデジタルＡＶデータを通常のデジタルＡＶデータに復号する。ここで、利用するデータが、コンテンツ重要度の高いデータ１（例えば、映画など）から低いデータ２（例えば、スポーツ番組など）に変化、あるいは変更する場合は、最初に受け取った各Ｋexの中から、必要なＫexを選択してＫcoを算出して用いることができるので、新たな認証手続きは勿論、Ｋexの要求もする必要が無い。

【００８９】前述の方法は、認証手続きに続いて入手可能な全てのＫexを一度に取得する方法であったが、図１２に示すような方法を用いてもよい。

【００９０】図１２において、まず、受信ユニット１３０では、要求レベル決定手段１３４が受信データのコンテンツ重要度に基づいて要求する認証のレベルを決定し、認証手段１３３に渡す。認証手段１３３はＤ－Ｉ／Ｆ１３１を介して送信ユニットに認証要求を出す。ここでは、一番高いレベルの認証を要求するものとする。送信ユニット１１１では、Ｄ－Ｉ／Ｆ１２３を介して受け取った認証要求に基づいて認証処理を行う。認証の方法については、例えば前述した実施の形態で説明した方法等により行うことができ、このとき送信ユニット、受信ユニットともに共有の共通鍵Ｋabが得られる。又、このときの認証済みのレベルがレベル判定手段１２２に渡される。

【００９１】次に、認証が完了してその通知が受信ユニット１３０に送信されると、認証手段１３３は、送信ユニット１１１に対して認証レベルが一番高いＫexを要求する。ここでは、Ｋexのレベルとして、高い順にｃｏｐｙ＿ｎｅｖｅｒ用（Ｋex1）、ｃｏｐｙ＿ｏｎｃｅ用（Ｋex2）、ｎｏ＿ｍｏｒｅ＿ｃｏｐｙ用（Ｋex3）の３種類とする。

【００９２】送信ユニット１１１では、レベル判定手段１２２が、認証手段１２１から受けた要求レベルを認証済みレベルに基づいて判定し、渡せるか否かの判定と、渡せる場合は、要求のあったＫex（このときは、Ｋex1）を両者が共有するＫabで暗号化して、認証手段１２１を通じて受信ユニット１３０に送信する。受信ユニット１３０では、認証手段１３３が暗号化されたＫab（Ｋex1）を自身の持つＫabで復号してＫex記憶手段１３７に記憶する。

【００９３】次に、受信ユニット１３０では、種要求コマンド発行手段１３５が種要求コマンドを送信ユニット１１１に送信する。そうすると、送信ユニット１１１では、種要求コマンド応答手段１２０が、種記憶手段１１８から種を取り出し受信ユニット１３０に送信する。

【００９４】種を受信した受信ユニット１３０では、種要求コマンド発行手段１３５が送信ユニット１１１から

受け取った種と、Kex記憶手段に記憶している復号化するデータのレベルに対応するKex（Kex1 ）とを用いて、Kco算出手段１３６は、送信ユニット１１１と同一の関数（この関数は、送信ユニット及び受信ユニットが予め持っており、第３者は入手できないものとする）によりKco（Kco1 ）を算出する。復号化手段１３２はこの算出されたKco1 を用いて暗号化されたデジタルＡＶデータを通常のデジタルＡＶデータに復号する。ここで、利用するデータが、コンテンツ重要度の高いデータ１から低いデータ２に変化、あるいは変更する場合は、別のKex（図ではKex2）を送信ユニット１１１に対して要求する。

【００９５】送信ユニット１１１では、レベル判定手段１２２が認証手段１２１を介して、要求されたKexのレベルを認証済みのレベルに基づいて判定し、認証済みレベルと同等か、あるいはそれより低いレベルの要求であれば、要求されたKex（Kex2）をKabで暗号化して受信ユニット１３０に送信する。

【００９６】ここで、受信ユニット１３０が、最初の認証要求を行って認証が完了した場合に、その認証済みのレベル（認証済みのレベルのうち最高のレベルのものでよい）を記憶しておき、次回からのKexの要求に対しては、その記憶した認証済みのレベルから所望するKexが認証無しに入手可能か否かを、例えば認証手段１３３で判断して入手可能であればKexを要求するようにしてもよい。このとき、入手不可能である場合は、更に、新たな高いレベルの認証を行うようにすればよい。従って、要求レベル決定手段１３４で、デジタルＡＶデータのコンテンツ重要度に基づいて決定された要求レベルが、記憶されている過去の認証済みレベルと同等かあるいはそれ以下のレベルである場合に、認証手段１３３から所望のKexを要求する。

【００９７】また、送信ユニット１１１側については、もし、認証要求がなくKexの要求があって、要求されたKexが送信不可と判定された場合に、新たな認証が必要である旨の情報を受信ユニット１３０側に通知する方法としてもよい。

【００９８】受信ユニット１３０では、認証手段１３３がKab（Kex2 ）を復号してKex記憶手段１３７に記憶し、Kco算出手段１３６がそのKex2及び種を用いてKco2を算出してデータを復号する。この方法によると、１度あるレベルでの認証が済んでいれば、そのレベルと同等か、あるいはそれ以下のレベルのKexを取得する場合、新たに認証手続きを行う必要が無いので、時間のかかる認証手続きの回数を減少することになる。

【００９９】ところで、従来のように、コンテンツの重要度の異なるＡＶデータを利用したい場合に、その都度認証手続きを行う方法では、受信ユニットが多数接続されているときは、認証要求の頻度が増大する。しかしながら、認証要求のための通信は、例えば、ＩＥＥＥ１３９４ＢＵＳ規格のようなアイソクロナスデータ通信とアシンクロナスデータ通信とを用いるものでは、本来データの通信帯域に使う帯域の一部を用いて行っているため、時間のかかる認証要求の頻度が増大することは好ましくない。従って、本実施の形態によれば、受信ユニットの台数が増えても、基本的には１受信ユニットについて１回の認証手続きで済むので、認証要求による不都合が生じない。

【０１００】なお、上記第五の実施の形態では、認証手続きのレベルを２段階としたが、これに限定されるものではない。

【０１０１】また、上記第五の実施の形態では、コンテンツの重要度のレベルを３種類としたが、これに限定されるものではない。例えば、ｃｏｐｙ＿ｆｒｅｅ（何度でも記録してよいコンテンツ）のレベルを加えて４種類としてもよいし、それ以上の種類としてもよい。

【０１０２】また、上記第五の実施の形態では、種と暗号鍵とを用いて関数により暗号化用の鍵を算出する方法により実現する構成としたが、これに限らず、他の実施の形態で説明した方法を用いた構成に適用してもよい。

【０１０３】また、上記第五の実施の形態では、受信中のデータの重要度を見て、要求するKexの種類を決定しているが、予め自分が受信する可能性のある全てのKexを取得しておいてもよい。

【０１０４】また、上記第五の実施の形態では、認証を行った後に、受信ユニットがKexの要求を行うとしたが、これに限定されない。例えば、認証要求をする際に、同時に自分が受け取りたいKexの種類を送信ユニットに対して申請し、認証が完了した時点で、送信ユニットが自動的に要求されたKexを受信ユニットに送信してもよい。

【０１０５】また、上記第五の実施の形態では、データの重要度に応じて暗号鍵を替える方法であったが、これに限らず、データの種類等に応じて暗号鍵を替えるようにしてもよい。その場合は、認証のレベルとデータの種類（すなわち、暗号鍵）を対応させておく必要がある。

【０１０６】次に本発明の第六の実施の形態について説明する。

【０１０７】図１３は、本発明の第六の実施の形態についての概略図である。本実施の形態は、Ｆｕｌｌ認証とＲｅｓｔｒｉｃｔｅｄ認証（以下，Ｒｅｓｔ認証と略称する）機能を備えたデジタルＡＶデータ送信ユニット１４０には、Ｒｅｓｔ認証機能のみを持つデジタルＡＶデータ受信ユニット１５０及びＦｕｌｌ認証とＲｅｓｔ認証の両機能を備えたデジタルＡＶデータ受信ユニット１６０が接続されているものとする。ここで、Ｆｕｌｌ認証とは、例えば公開鍵と秘密鍵とを用いた高レベルの認証方法であり、Ｒｅｓｔ認証とは、例えば共通鍵を用いた通常の認証方法を示すものとする。

【０１０８】図１３において、デジタルＡＶデータ送信

ユニット１４０は、データを暗号化する暗号化手段１４１、Ｆｕｌｌ認証用のルールを格納するＦｕｌｌ認証格納手段１４３、Ｒｅｓｔ認証用のルールを格納するＲｅｓｔ認証格納手段１４２、管理基準としてのＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ ＲｅｖｏｃａｔｉｏｎＬｉｓｔ：不正機器の排除を行うための不正機器リスト）を格納するＣＲＬ格納手段１４４、受信ユニットからの認証要求を受けて認証ルールを選択する送信側認証選択手段１４７、その送信側認証選択手段１４７の選択結果に応じて、Ｆｕｌｌ認証とＲｅｓｔ認証を切り替える切替手段１４８、切り替えられて選択された認証ルールにより受信ユニットとの間で認証を行う認証手段１４６、及び受信ユニットとの間で暗号化データや認証要求など情報のやり取りを行うＤ－Ｉ／Ｆ（デジタルインターフェース）１４５から構成されている。ＣＲＬは入力データに付加されて新しい内容に随時更新される。

【０１０９】一方、デジタルＡＶデータ受信ユニット１５０は、送信ユニットとの間で暗号化データや認証要求など情報のやり取りを行うＤ－Ｉ／Ｆ１５１、送信ユニットから受信した暗号化データを復号化する復号化手段１５２、送信ユニットに対して認証要求を行う認証要求手段１５３、及びＲｅｓｔ認証ルールにより認証を行う認証手段１５４から構成されている。

【０１１０】また、デジタルＡＶデータ受信ユニット１６０は、送信ユニットとの間で暗号化データや認証要求など情報のやり取りを行うＤ－Ｉ／Ｆ１６１、送信ユニットから受信した暗号化データを復号化する復号化手段１６２、送信ユニットに対して認証要求を行う認証要求手段１６３、Ｆｕｌｌ認証用のルールを格納するＦｕｌｌ認証格納手段１６６、Ｒｅｓｔ認証用のルールを格納するＲｅｓｔ認証格納手段１６５、認証要求手段１６３からの指示により認証ルールを切り替える切替手段１６７、及び切り替えられ選択された認証ルールにより認証を行う認証手段１６４から構成されている。

【０１１１】次に、上記実施の形態の動作について図面を参照しながら説明する。

【０１１２】まず、前述のＣＲＬは、管理センターから送られてくるが、入手するには、Ｆｕｌｌ認証の機能を利用する。そのため、Ｒｅｓｔ認証機能のみを持つ機器では、ＣＲＬを入手できない。従って、Ｒｅｓｔ認証機能のみを持つ機器側は、ＣＲＬチェックによる機器排除を行えない。ここで、送信ユニット及び受信ユニットがともにＦｕｌｌ認証及びＲｅｓｔ認証機能を有する場合について、ＣＲＬチェックを用いた手順を説明する。

【０１１３】図１５は、図４に示した公開鍵及び秘密鍵による認証方法に、ＣＲＬチェックを付加したものである。

【０１１４】図１５において、送信側には、管理センター（ライセンス機構）からそのユニットの識別用のＩＤａ、及びそのＩＤａに対する署名Ａが送られ、受信側には、管理センターからそのユニットの識別用のＩＤｂ、及びそのＩＤｂに対する署名Ｂが送られているものとする。また、この場合受信側は秘密鍵Ｓｂと公開鍵Ｐｂを持つ。また送信側は秘密鍵Ｓａと公開鍵Ｐａを持つ。

【０１１５】まず、ステップ４１で受信側が乱数Ｂを発生する。受信側は自己の認識番号であるＩＤｂ及び署名Ｂと、乱数Ｂを自らの秘密鍵Ｓｂで暗号化した暗号文Ｓｂ（Ｂ）を送信側に送る。送信側は受信側の認識番号ＩＤｂから検索して受信側の公開鍵Ｐｂを入手する。ステップ４９で、入手した公開鍵Ｐｂで暗号文Ｓｂ（Ｂ）を復号化する。その結果ステップ５０のごとく乱数Ｂが得られる。さらに、送信側は、ステップ５１で、受信側のＩＤｂに対してＣＲＬチェックを行う。すなわち、ＩＤｂがＣＲＬに無いかどうかを調べ、無ければステップ５２で乱数Ａを発生する。ＣＲＬに有れば不正機器であるとして認証を中止する。ステップ５２で、乱数ＡとＢは送信側の秘密鍵Ｓａで暗号化され暗号文Ｓａ（Ａ，Ｂ）が作成される。送信側は暗号文Ｓａ（Ａ，Ｂ）と自己の認識番号ＩＤａを受信側に送信する。受信側は、暗号文Ｓａ（Ａ，Ｂ）と送信側の認識番号ＩＤａを受け取り、送信側の認識番号ＩＤａから検索して送信側の公開鍵Ｐａを入手し、ステップ４２のごとく、Ｐａで暗号文Ｓａ（Ａ，Ｂ）を復号化する。ここで、暗号文Ｓａ（Ａ，Ｂ）から受信側にはステップ４１で送った乱数Ｂと全く同一の乱数Ｂが得られ、偽造や改竄が行われてないことが受信側にわかる。もし前記２つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。但し、この場合は、公開鍵Ｐａ，Ｐｂは正当な者にしか入手できないようになっているものとする。次に受信側はステップ４３のごとく、受信側の秘密鍵Ｓｂで乱数Ａを暗号化し、暗号文Ｓｂ（Ａ）を作成する。Ｓｂ（Ａ）は送信側に送られ、ステップ５３のごとく既に送信側で持っている、受信側の公開鍵Ｐｂで暗号文Ｓｂ（Ａ）を復号化する。ステップ５２で発生した、乱数Ａとステップ５３で復号化した乱数Ａが全く同一であれば、偽造や改竄が行われていないことが送信側にわかる。もし前記２つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。

【０１１６】一方、受信側は、ステップ４４で送信側のＩＤａに対してＣＲＬチェックを行う。そして、ＩＤａがＣＲＬに有れば認証を中止し、無ければ次のステップに移る。今、送信側及び受信側でのＣＲＬチェックの結果が異常が無く、受信側と送信側でやりとりした乱数ＡとＢは偽造や改竄が行われていないとすると、受信側と送信側以外の第３者には乱数ＡとＢは秘密の乱数である。そこで送信側で、ステップ５４のごとく、乱数ＡとＢを用いて鍵Ｋａｂを作成する。同じくステップ４５のごとく受信側で乱数ＡとＢを用いて鍵Ｋａｂを作成する。前記２つのＫａｂは全く同一のものであり共通鍵と

なっている。次に送信側でステップ５５のごとく鍵Ｋexを作成する。これを共通鍵Ｋａｂで暗号化し、暗号文Ｋａｂ（Ｋex）を作成して、受信側に送る。受信側はステップ４６のごとく共通鍵Ｋａｂで暗号文Ｋａｂ（Ｋex）を復号化してＫexを得、その結果、受信側が得た鍵Ｋexと送信側にある鍵Ｋexは全く同一であり、共通鍵となる。次に送信側でステップ５６のごとく鍵Ｋcoを作成する。鍵Ｋcoは共通鍵Ｋexで暗号化され、暗号文Ｋex（Ｋco）として、受信側に送られる。受信側では、ステップ４７のごとく共通鍵Ｋexで暗号文Ｋex（Ｋco）を復号化し、ステップ４８のごとくＫcoを得る。送信側にある鍵Ｋcoと受信側にあるＫcoは全く同一で、共通鍵となっている。以上が公開鍵と秘密鍵による認証の過程で得られたワーク鍵Ｋcoである。

【０１１７】上記説明では、ＣＲＬチェックをステップ５２の乱数Ａの発生の前に行ったが、ＩＤｂ受信後であれば、どこで行ってもよい。規格上はKABを作成するステップ５４の後に行う。

【０１１８】次に、受信側がＲｅｓｔ認証機能のみの場合について説明する。この共通鍵による認証を行う場合は、前述したような方法を用いることはできない。そこで、受信側にそのユニットに対するＣＲＬ用のＩＤとそのＩＤを用いて作成された署名を付与し、送信側でＣＲＬを利用する方法を用いる。

【０１１９】図１４において、受信側には、管理センターから受信ユニットのＩＤｂ及び署名Ｂが与えられ、送信側と受信側は共通鍵Ｓを持つ。なお、この共通鍵は正当な者にしか与えられていない。まず、受信側でステップ３０のごとく２個の乱数Ａ１，Ａ２を発生し、共通鍵Ｓで暗号化し、暗号文Ｓ（Ａ１Ａ２）を作成し、ＩＤｂ及び署名Ｂとともに送信側へ送る。送信側ではステップ３５のごとく共通鍵Ｓで暗号文Ｓ（Ａ１Ａ２）を復号化する。そして、受信側のＩＤｂに対してＣＲＬチェックを行う。また、署名Ｂもチェックする。このとき、ＣＲＬチェック及び署名Ｂのチェックのどちらか一方でも異常が有る場合は、認証を中止する。ＣＲＬチェック及び署名Ｂのチェックの結果が両方とも正常であれば、ステップ３７のごとく乱数Ａ１と乱数Ａ２が得られる。送信側は乱数Ａ２を受信側に送る。受信側はステップ３１のごとく２つの乱数Ａ１とＡ２を持つことになる。ステップ３０で発生した乱数Ａ２とステップ３１で送信側から受け取った乱数Ａ２が全く同じであれば、送信側で偽造や改竄が行われていないことがわかる。もし、上記２つの乱数が異なっていれば偽造や改竄が行われたことになり認証は失敗する。次に送信側はステップ３８のごとく乱数Ｂ１とＢ２を発生し、暗号化して、暗号文Ｓ（Ｂ１Ｂ２）を受信側に送る。受信側はステップ３２のごとく共通鍵Ｓを用いて暗号文Ｓ（Ｂ１Ｂ２）を復号化する。すると、ステップ３３のごとく乱数Ｂ１とＢ２が得られる。受信側は乱数Ｂ２を送信側に送る。送信側はステップ３９のごとく乱数Ｂ１とＢ２を持つことになる。ステップ３８で発生した乱数Ｂ２と、ステップ３９で受信側から受け取った乱数Ｂ２が同じであれば、受信側に、偽造や改竄が行われていないことがわかり、認証は成功する。もし、上記２つの乱数が異なっていれば、偽造や改竄が行われたことになり認証は失敗である。

【０１２０】ここまでで、認証が成功しているとすると、乱数Ａ１と乱数Ｂ１は送信側と受信側以外の第３者には秘密の乱数である。送信側ではステップ４０のごとくＩＤｂ及び乱数Ａ１と乱数Ｂ1から鍵Ｋcoを作成する。一方受信側では、ステップ３４のごとくＩＤｂ及び乱数Ａ１と乱数Ｂ１から鍵Ｋcoを作成する。送信側にある鍵Ｋcoと受信側にある鍵Ｋcoは全く同一であり、共通鍵となっている。以上が共通鍵による認証の過程で得られたワーク鍵Ｋcoである。この方法によれば、ＩＤｂと署名Ｂが対応しているので、ＩＤｂが盗まれて送信側でのＣＲＬチェックがパスしても、署名Ｂによるチェックで不正使用が防止できる。

【０１２１】ここで、ＣＲＬ用のＩＤは、例えば４０ビットのデバイスＩＤを使用する。これにより、Ｆｕｌｌ認証、Ｒｅｓｔ認証に関わらずすべての１３９４ＣＰデバイスが４０ビットのデバイスＩＤを持つことになる。

【０１２２】なお、上記の説明では、管理センターでの署名の作成を、ＩＤを用いて作成したが、このＩＤは管理センターが任意に決めるものである。さらに、安全性を高めるために、機器を製作する時に予め機器毎に埋め込まれる機器固有の識別子であるＮＵＩＤを用いる。すなわち、受信側は管理センターに申請する際に、その機器のＮＵＩＤを知らせ、管理センターは、そのＮＵＩＤとＣＲＬ用のＩＤを用いて署名を作成し、ＣＲＬ用のＩＤと署名を受信側に付与する。

【０１２３】また、上記実施の形態では、認証ルールの種類をＦｕｌｌとＲｅｓｔの２種類としたが、認証ルールの種類はこれに限定されるものではなく、３種類以上であっても、受信側がＣＲＬを持てない機器構成の場合は、前述と同様に適用可能である。

【０１２４】また、本発明の各構成要素は、それぞれの機能を実現する専用のハード回路、機器等で実現しても、あるいは、コンピュータを利用してソフトウェア的に実現してもかまわない。

【０１２５】また、本発明をコンピュータで実現する場合、それらの各構成要素の機能の全部又は一部を実現するためのプログラムを格納した媒体も本発明に属する。

【０１２６】

【発明の効果】以上説明したところから明らかなように、本発明は、重要でないデータの認証に多くの時間を要せず、重要なデータに関しては、その認証が偽造や改竄に強くまた、ユニットによって認証に必要な厳密さを変えることによって、データの重要性や相手の装置が有する認証方法の種別などを考慮して、適切な認証方法で

データの送受信を行いうるユニット、システム等を提供することができる。

【０１２７】また、本発明は、コンテンツの重要度に応じた複数種類の解読情報を得る場合に、認証回数を減少することができるという利点がある。

【０１２８】また、本発明は、排除機能を持たない受信機器であっても、送信側で機器の排除を行うことが可能となる。

【図面の簡単な説明】

【図１】本発明の第一の実施の形態についての概略図

【図２】従来技術について示す概略図

【図３】従来技術について示す概略図

【図４】本発明の実施の形態のうち認証方法に関するブロック図

【図５】本発明の実施の形態のうち認証方法に関するブロック図

【図６】本発明の第二の実施の形態についての概略図

【図７】本発明の第三の実施の形態についての概略図

【図８】本発明の第四の実施の形態についての概略図

【図９】本発明の第四の実施の形態についての概略図

【図１０】本発明の第五の実施の形態についての概略図

【図１１】同第五の実施の形態における手順方法の一例を示す図

【図１２】同第五の実施の形態における手順方法の別の一例を示す図

【図１３】本発明の第六の実施の形態についての概略図

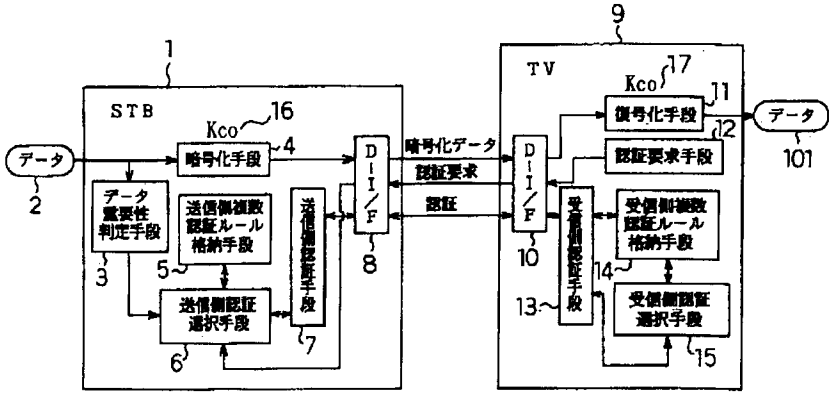
【図１４】同第六の実施の形態における手順方法の一例を示す図

【図１５】送信側及び受信側両方でＣＲＬチェックを行う場合の手順方法の一例を示す図

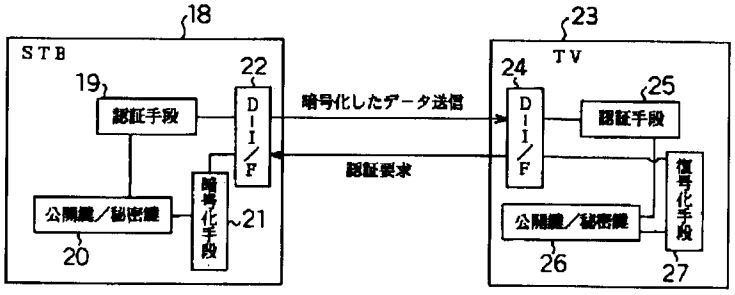
【符号の説明】

１　ＳＴＢ
３　データ重要性判定手段
５　送信側複数認証ルール格納手段
６　送信側認証選択手段
７　送信側認証手段
９　ＴＶ
１３　受信側認証手段
１４　受信側複数認証ルール格納手段
１５　受信側認証選択手段
１８　ＳＴＢ
１９　認証手段
２０　公開鍵／秘密鍵
２３　ＴＶ
２５　認証手段
２６　公開鍵／秘密鍵
２８　ＳＴＢ
２９　認証手段
３０　共通鍵
３３　ＴＶ
３５　認証手段
３６　共通鍵
３８　ＳＴＢ
４１　送信側複数認証ルール格納手段
４２　ユニット認証ルール情報受信手段
４３　送信側認証手段
４５　ＶＴＲ
４８　認証要求手段
４９　受信側認証ルール格納手段
５０　認証ルール情報送信手段
５１　受信側認証手段
５５　送信側認証ルール取り出し手段
５６　ＳＴＢ
５７　データ重要性判定手段
５８　送信側認証ルール取り出し手段
５９　送信側認証選択手段
６０　ユニット認証ルール情報受信手段
６１　送信側認証手段
６３　送信側複数認証ルール格納手段
６５　ＴＶ
６７　認証要求手段
６８　受信側複数認証ルール格納手段
６９　受信側認証選択手段
７０　受信側認証手段
７２　ＶＴＲ
７４　認証要求手段
７５　受信側認証ルール格納手段
７６　認証ルール情報送信手段
７７　受信側認証手段
８６　データ重要性判定手段
８７　管理基準参照決定手段
８８　管理基準格納手段
８９　認証決定手段
９０　認証手段
９２　ＴＶ
９３　ＳＴＢ
９４　ＳＴＢ
９５　管理基準参照決定手段
９６　管理基準格納手段
９７　認証決定手段
９８　認証手段
１００　ＶＴＲ
１４４　ＣＲＬ格納手段

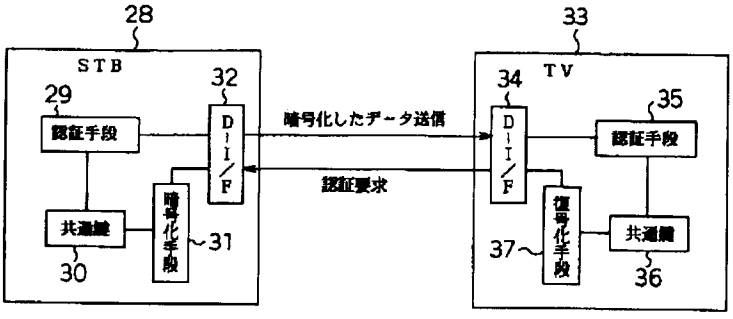
【図１】


STB
TV
データ
暗号化手段
Kco
暗号化データ
認証要求
認証
D I / F
データ重要性判定手段
送信側複数認証ルール格納手段
送信側認証手段
送信側認証選択手段
復号化手段
認証要求手段
受信側複数認証ルール格納手段
受信側認証手段
受信側認証選択手段
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
101

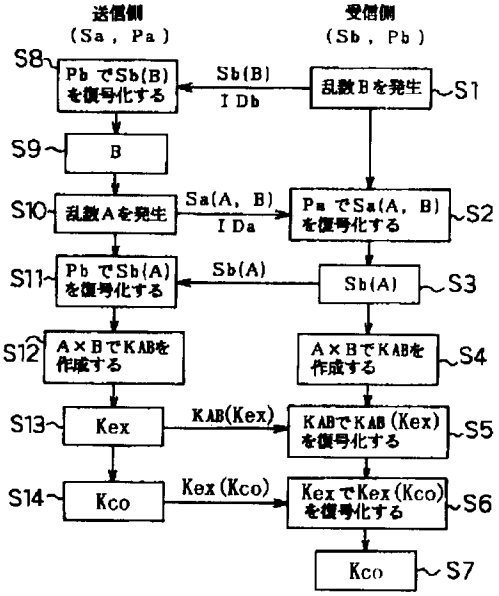
【図２】


STB
TV
認証手段
公開鍵／秘密鍵
暗号化手段
D I / F
暗号化したデータ送信
認証要求
復号化手段
18
19
20
21
22
23
24
25
26
27

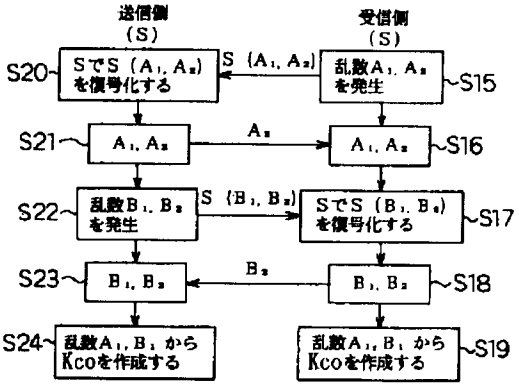
【図３】


STB
TV
認証手段
共通鍵
暗号化手段
D I / F
暗号化したデータ送信
認証要求
復号化手段
28
29
30
31
32
33
34
35
36
37

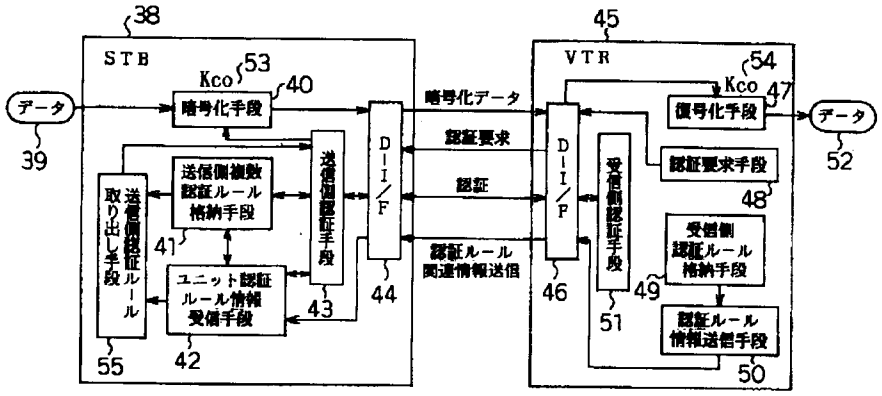
【図４】


送信側
(Sa , Pa)
受信側
(Sb , Pb)
S8
Pb でSb(B)を復号化する
Sb(B) IDb
乱数Bを発生
S1
S9
B
S10
乱数Aを発生
Sa(A, B) IDa
Pa でSa(A, B)を復号化する
S2
S11
Pb でSb(A)を復号化する
Sb(A)
Sb(A)
S3
S12
A×BでKABを作成する
A×BでKABを作成する
S4
S13
Kex
KAB(Kex)
KABでKAB(Kex)を復号化する
S5
S14
Kco
Kex(Kco)
KexでKex(Kco)を復号化する
S6
Kco
S7

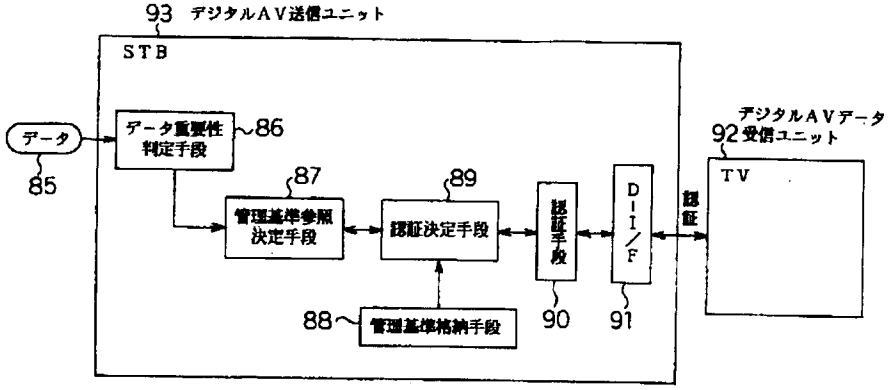
【図５】


送信側
(S)
受信側
(S)
S20
SでS (A1, A2)を復号化する
S (A1, A2)
乱数A1, A2を発生
S15
S21
A1, A2
A2
A1, A2
S16
S22
乱数B1, B2を発生
S (B1, B2)
SでS (B1, B2)を復号化する
S17
S23
B1, B2
B2
B1, B2
S18
S24
乱数A1, B1 からKcoを作成する
乱数A1, B1 からKcoを作成する
S19

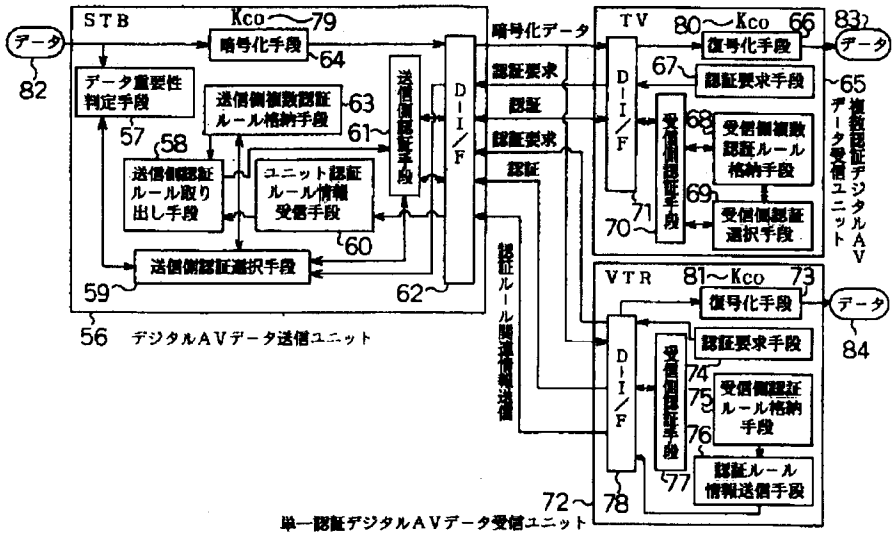
【図６】


38
STB
Kco
53
40
データ
39
暗号化手段
暗号化データ
認証要求
認証
認証ルール関連情報送信
送信側複数認証ルール格納手段
41
送信側認証ルール取り出し手段
ユニット認証ルール情報受信手段
42
43
送信側認証手段
D I／F
44
45
VTR
54
Kco
47
復号化手段
データ
52
認証要求手段
48
受信側認証ルール格納手段
受信側認証手段
49
51
D I／F
46
認証ルール情報送信手段
50
55

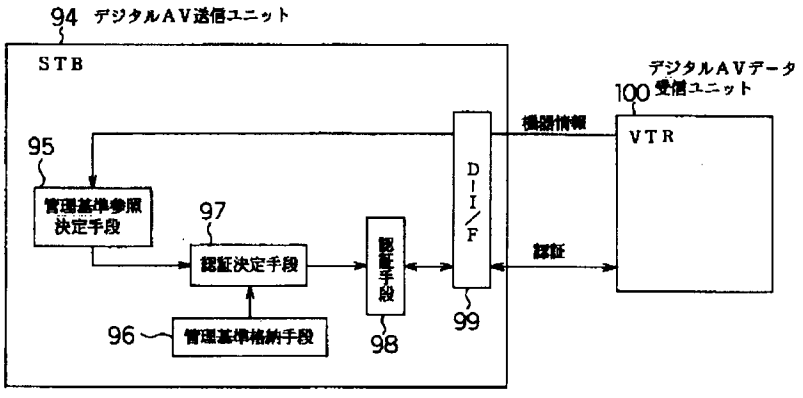
【図８】


93 デジタルＡＶ送信ユニット
STB
データ
85
データ重要性判定手段
86
87
管理基準参照決定手段
89
認証決定手段
88
管理基準格納手段
認証手段
90
D I／F
91
認証
デジタルＡＶデータ
92 受信ユニット
TV

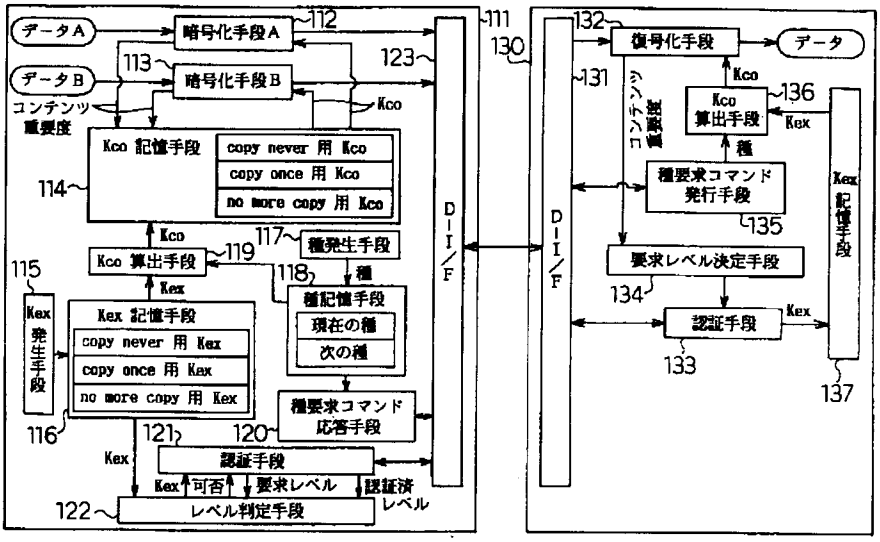
【図７】


STB
Kco
79
データ
暗号化手段
64
82
データ重要性判定手段
57
送信側複数認証ルール格納手段
63
58
61
送信側認証ルール取り出し手段
ユニット認証ルール情報受信手段
60
送信側認証手段
送信側認証選択手段
59
62
D I／F
56
デジタルＡＶデータ送信ユニット
暗号化データ
認証要求
認証
認証要求
認証
認証ルール関連情報送信
TV
80
Kco
66
復号化手段
83
データ
67
認証要求手段
65
D I／F
受信側認証手段
68
受信側複数認証ルール格納手段
69
受信側認証選択手段
70
71
複数認証デジタルＡＶデータ受信ユニット
VTR
81
Kco
73
復号化手段
データ
84
認証要求手段
74
D I／F
受信側認証手段
75
受信側認証ルール格納手段
76
77
認証ルール情報送信手段
72
78
単一認証デジタルＡＶデータ受信ユニット

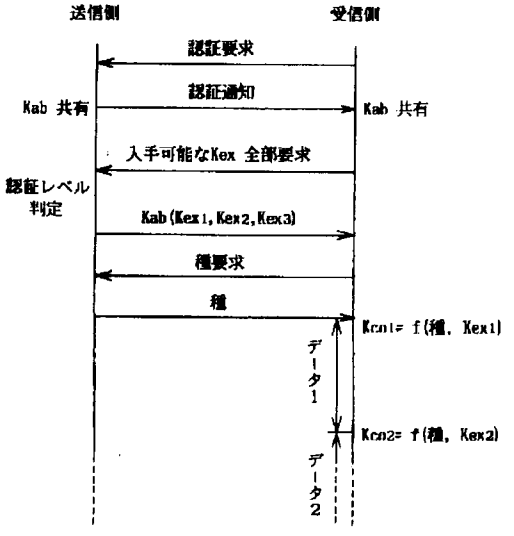
【図９】


94
デジタルＡＶ送信ユニット
STB
デジタルＡＶデータ
100
受信ユニット
機器情報
VTR
95
管理基準参照決定手段
97
認証決定手段
認証手段
D I／F
認証
96
管理基準格納手段
98
99

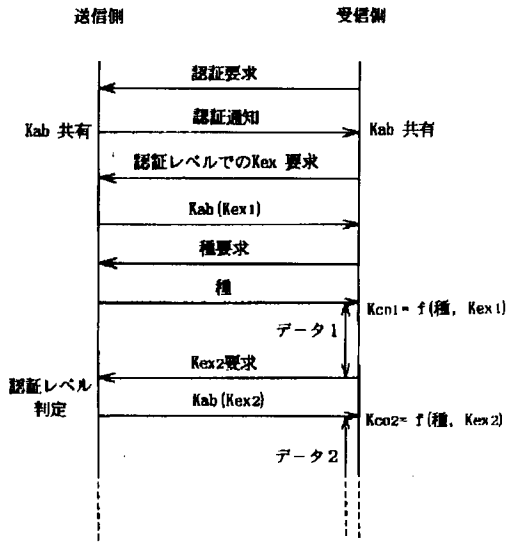
【図１０】


データA
暗号化手段A
112
111
130
データB
113
暗号化手段B
123
Kco
コンテンツ重要度
Kco 記憶手段
copy never 用 Kco
copy once 用 Kco
no more copy 用 Kco
114
D I / F
Kco
Kco 算出手段
119
117
種発生手段
118
種
115
Kex
Kex 発生手段
Kex 記憶手段
copy never 用 Kex
copy once 用 Kex
no more copy 用 Kex
116
種記憶手段
現在の種
次の種
種要求コマンド応答手段
121
120
Kex
認証手段
Kex
可否
要求レベル
認証済レベル
122
レベル判定手段
132
復号化手段
データ
Kco
131
コンテンツ重要度
Kco 算出手段
136
Kex
種
種要求コマンド発行手段
135
要求レベル決定手段
134
認証手段
Kex
133
Kex 記憶手段
137

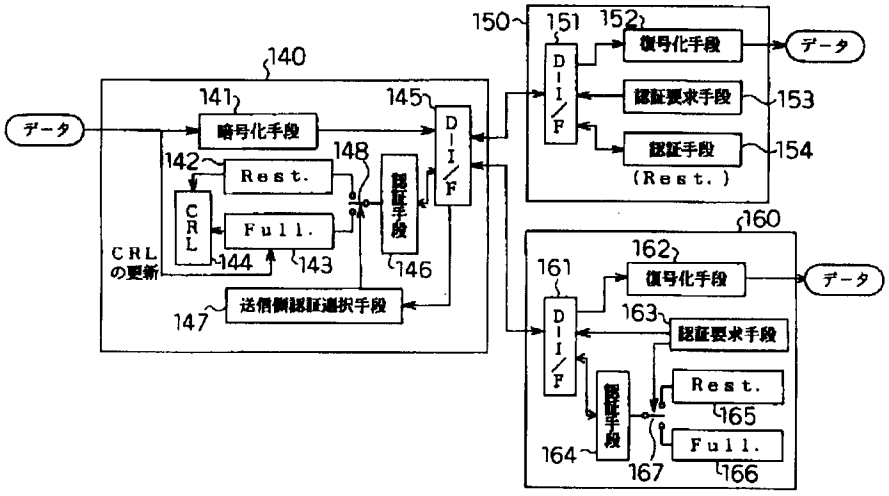
【図１１】


送信側
受信側
認証要求
認証通知
Kab 共有
Kab 共有
入手可能なKex 全部要求
認証レベル判定
Kab(Kex1, Kex2, Kex3)
種要求
種
Kco1= f(種, Kex1)
データ1
Kco2= f(種, Kex2)
データ2

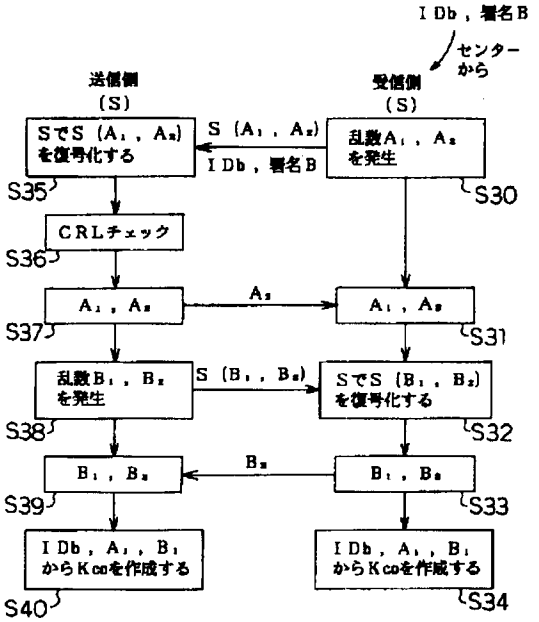
【図１２】


送信側
受信側
認証要求
認証通知
Kab 共有
Kab 共有
認証レベルでのKex 要求
Kab(Kex1)
種要求
種
Kco1= f(種, Kex1)
データ1
Kex2要求
認証レベル判定
Kab(Kex2)
Kco2= f(種, Kex2)
データ2

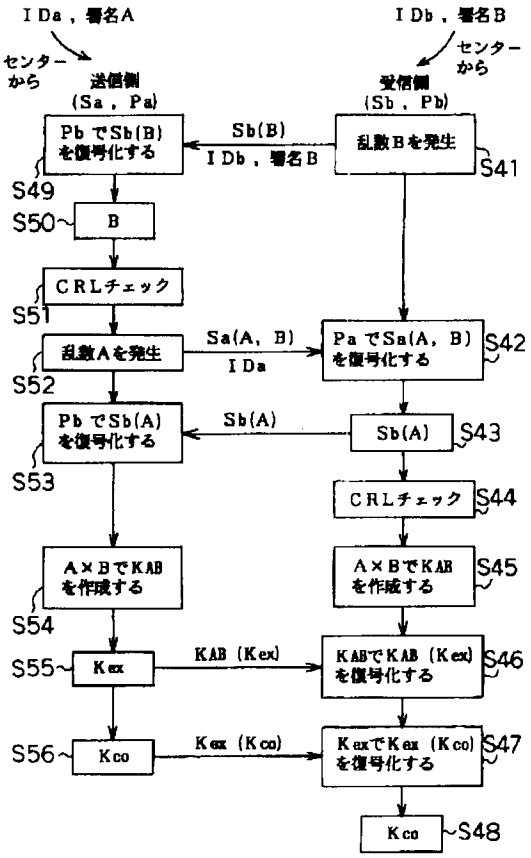
【図１３】


150
151
152
復号化手段
データ
D I / F
認証要求手段
153
認証手段
154
(Rest.)
140
141
暗号化手段
145
D I / F
データ
142
Rest.
148
認証手段
CRL
Full.
CRL の更新
144
143
146
送信側認証選択手段
147
160
162
復号化手段
データ
161
D I / F
163
認証要求手段
Rest.
165
認証手段
164
167
Full.
166

【図１４】


I Db , 署名B
センターから
送信側 (S)
受信側 (S)
SでS (A1 , A2) を復号化する
S (A1 , A2)
I Db , 署名B
乱数A1 , A2 を発生
S35
S30
CRLチェック
S36
A1 , A2
A2
A1 , A2
S37
S31
乱数B1 , B2 を発生
S (B1 , B2)
SでS (B1 , B2) を復号化する
S38
S32
B1 , B2
B2
B1 , B2
S39
S33
I Db , A1 , B1 からKcoを作成する
I Db , A1 , B1 からKcoを作成する
S40
S34

【図１５】


I Da , 署名A
センターから
送信側 (Sa , Pa)
Pb でSb(B) を復号化する
S49
S50
B
CRLチェック
S51
乱数Aを発生
S52
Pb でSb(A) を復号化する
S53
A×BでKABを作成する
S54
S55
Kex
S56
Kco
I Db , 署名B
センターから
受信側 (Sb , Pb)
Sb(B)
I Db , 署名B
乱数Bを発生
S41
Sa(A, B)
I Da
Pa でSa(A, B) を復号化する
S42
Sb(A)
Sb(A)
S43
CRLチェック
S44
A×BでKABを作成する
S45
KAB (Kex)
KABでKAB (Kex) を復号化する
S46
Kex (Kco)
KexでKex (Kco) を復号化する
S47
Kco
S48

フロントページの続き

(72)発明者　山田　正純
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　後藤　昌一
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　武知　秀明
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　臼木　直司
大阪府門真市大字門真1006番地　松下電器産業株式会社内